Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Instant War, Just Add Chat: The Growth of Instant Messaging Technology

Just as there was a steadily growing war for dominance between Web-Browsers during the 1990's, there has been a similar battle within the microcosm of the Instant Messaging (IM) world. And like the larger browser war, the area of IM technologies has had a snowball beginning, a proliferation of initial players and capabilities, large corporations playing hardball politics with their popularity strategies, and, as with every new freedom or technology, new areas for potential risks. In the following discussion, the backgr...

Copyright SANS Institute

Author Retains Full Rights

AD

An Instant War, Just Add Chat
- **The Growth of Instant Messaging Technology**

Just as there was a steadily growing war for dominance between Web-Browsers during the 1990's, there has been a similar battle within the microcosm of the Instant Messaging (IM) world. And like the larger browser war, the area of IM technologies has had a snowball beginning, a proliferation of initial players and capabilities, large corporations playing hardball politics with their popularity strategies, and, as with every new freedom or technology, new areas for potential risks. In the following discussion, the background, major players, IM capabilities, competitive environment, security issues, recommended solutions, and future outlook will be explored. The purpose of the information presented here is to provide the reader with a rich synthesis of observations and ideas, encourage the reader to evaluate their current technological environment, and spur one to explore what additional work may need to be done in this security issue.

Background

The advent of IM technology began in July of 1996 with the creation of Mirabilis Ltd. by four Israeli Internet users. Mirabilis was created to meet the need of a growing Internet community who was "connected- but not interconnected". The technology was designed to allow users to locate and exchange communications over the vast Internet landscape with other users via peer-to-peer connections. In November of 1996 the first version of ICQ (I-Seek-You) was released and quickly notched out a new category in the virtual world. Being the first Internet-based chat application allowed ICQ to be the tool that would allow Mirabilis to form a new philosophy in how people locate each other, program propagation, features, functionality, and even terminology. Due to ICQ, Mirabilis also produced a proprietary, robust Internet server technology with an upscalable architecture. ICQ's growth was so monumental that within half of a year there were almost a million registrations.

Figure A *to the right provides a breakdown of how this technology is being used in companies.*

Figure A:
"Most organizations aren't using IM" June 12, 2001
TechRepublic Staff

Since its beginnings, ICQ has developed into more than simple instant messages, now there are user-created interest lists, public chat-rooms, new clients and enhancements, virtual communities, and its own Intranet Server for enterprises soon followed. SMS is an IM solution that developed in Europe as the European answer to mainstream IM products. However, in June of 1998, Mirabilis' assets were acquired

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

by America Online (AOL) and the result is today's ICQ Inc. The complete history of this phenomenon can be read at www.icq.com in the "About Us" section. This leads us to the next area of interest, the players that are now performing in this arena, no matter how small it looks.

Players

The two largest armies on the IM battlefield are AOL and Microsoft. AOL had about eighty-percent of the market with its ICQ and Instant Messenger products. Microsoft has its IM version called MSN Messenger, and corporate tool called NetMeeting. There is a number of medium to small sized competitors also. Yahoo Messenger has a fairly large market share behind MSN Messenger. IBM's Lotus application Lotus SameTime is one of the few products that is not subscription-based, but is an actual purchase product. Some of the smaller operators include: NovaWiz's Odigo, eShare, PeopleLink, iChat's Pager, Excite's PAL, Tribal Voice Software's PowWow, IMICI, and PHT's specifically designed LogPad for doctors to use with patients in clinical trials. Kyle Harmon gives a good comparison analysis of the most popular IM clients in his article "Instant Message Options for the Corporate Environment" on www.techrepublic.com. However, the IM battlefield is about to get more interesting with the advent of strategic alliances that will be discussed in the Competition section. In addition to the main "armies" and their alliances, there are external parties that are pairing up with IM providers to provide some of the added capabilities that will be explored in this next section.

Capabilities

> "In my line of work, using IM is the best thing since sliced bread," [Michael] Kaika said in an interview conducted via IM with Katie Dean. "Years ago, I had to rely on an interpreter to chat with media people. But now, rarely do I need to do that."
>
> Students often use instant messaging instead of Teletype machines (TTYs) connected to telephones to communicate with friends and relatives. "I am comfortable in saying that deaf people now rely on IM more than [on] TTYs," wrote Kiaka.
>
> (www.wired.com – "Instant Messaging Grows Up")

The above interview by Katie Dean underlines the capabilities that are being added by IM simply through new applications of the tool. Previously, a product by PHT was mentioned called LogPad that uses IM technology to send patient information to doctors when patients have an emergency. Dean goes on to point out that IM has become an invaluable tool for attorneys during negations, employees during phone interviews, and businessmen during meetings. These capabilities are only new applications of the IM tool. The potential for application of this tool will only be expanding exponentially with the expanding capabilities of the various IM tools.

The weapons of engagement are being improved as upstart companies bring them in with them as they join in the war hoping for a competitive advantage. Companies like FaceTime Communications Inc., Multimate (Instant Rendezvous Chat - CommTouch), and Cahoots have developed IM technologies that will integrate with company WebPages like Discovery Channel, Excite, Warner Bros., Ziff-Davis, and Alaska Airlines. These technologies may break down several barriers in that they are designed to allow users with various IM chat applications to chat together with interoperability, as well as chat with help desk personnel from the company's Web Page. The second barrier that may be broken down could be the traditional IM law that you must know a person and their contact information before you can talk with

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

them. These applications are designed to allow visitors to the same Web Page to discuss its contents even if they are not already set-up to talk to one another via the "Buddy List" style of pre-approved friends.

ActiveBuddy stated that it will provide real-time stock quotes via instant messenger "bots" for Nasdaq, NYSE, and AmEx with the aid of Reuters. This capability would allow users to send a company's name as a text message and receive a corresponding stock quote as a response. According to Stefanie Olsen in her article "IM Buddy Making More Powerful Friends" at news.cnet.com, ActiveBuddy has developed a natural-language search that uses scripts to communicate with databases. In addition, ActiveBuddy has a business model that includes marketing companies for event broadcast advertisements like album releases.

Independent programmers developed a product called Aimster that enables users to trade files in a much more secure manner than with the popular file-swapping software Napster. This program works over AOL's IM service. Message swapping has been a capability of IM programs for some time now, but Aimster provides search and retrieval functions that were not previously available on IM peer-to-peer networks (www.wired.com, "Wired News Report").

Telephony, or voice over the Internet, technology has been expanded with the voice communication capabilities of IM programs by using advanced compression techniques along with improved server capabilities (www.wired.com – Helft). Products like Voxware's VoxChat could be used for video-conferencing, voice-based chat groups, games, and distance learning. Some IM players have been working with translation capabilities for IM programs.

Microsoft acquired Flash Communications in 1998, and has been using this technology to add enhancements to MSN Messenger ever since. Along with this, a Chat component is available for the Exchange 2000 server as an enterprise solution for conferencing. This would allow users to record entire conferences for later use, have a conference meeting with more individuals than previously capable, and can be used by Tech Support to help network users.

Yahoo IM recently enhanced its messenger service to allow users to view each other as they communicate through the messenger client. Up until this point, many different forms of communication and communication media have been able to pass through the IM channel. Delivering live pictures was a significant step from text, pictures, voice, and other misc. files being sent via IM.

IM applications have also been developed for wireless communication with PDAs and the Blackberry devices. However, these capabilities rest only with AOL or CompuServe service users. This degree of separation in the capabilities listed thus far naturally lend to the next area of the war, and that is the Competition conflict itself between the players and their capabilities.

Competition

Even though most of the action in this battle has been fought in this area, competition looks more like a war of attrition in which both sides put in a lot of resources, but nobody gains any ground. The battle lines consist of AOL Time Warner and its two IM products, ICQ and IM, vs. the rest. There have also been tragedies due to this attrition style of battle; some of the upstart IM providers like PowWoW and iCast have had to discontinue service to users.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Messaging at Work and Play

More than half of all free instant messaging in January was through AOL's services.

SOURCE	HOME*	WORK*
AOL Instant Messenger	21.3	5.4
ICQ (owned by AOL)	8.5	1.2
Microsoft	13	2.7
Yahoo	10.4	1.9
TOTAL	53.2	11.2

*MILLIONS OF UNIQUE USERS. SOURCE: MEDIA METRIX

Figure B:
THE INDUSTRY STANDARD MAGAZINE
"Business Gets the Message"
February 26, 2001

Figure B *to the left provides a breakdown of how what portion of the IM market is using which IM product and where.*

AOL Time Warner has kept its products on a different channel than the rest of the IM products. Other IM products have adapted and evolved to be able to communicate with AOL's IM products a number of times. However, AOL Time Warner responds to each evolutionary cycle by reconfiguring its product and servers so that interoperability between AOL Time Warner's IMs and other IMs is no longer possible.

"The Rest" have attempted to find strength in numbers as competitors have banded together. One of the first alliances of this nature was in 1999 with Excite, Tribal Voice, Prodigy, Yahoo, AT&T, Infoseek, and Microsoft sat down to discuss solutions to the non-AOL user blockade. However, AOL returned fire by aligning the efforts of Sun Microsystems, RealNetworks, Novell, and Apple with its products. In February of 2001, Yahoo, Microsoft, AT&T, Excite@Home, Odigo, and Prodigy Communications came together to form IMUnified. The goal of this coalition is to be "committed to functional interoperability," said Estela Mendoza, an IMUnified spokeswoman. A protocol has already been developed. IMUnified has used its unified voice to petition its concern to the FCC and cast doubts upon AOL's privacy and security claims.

The Internet community has proved to be a fickle audience in this skirmish. When MSN Messenger services were halted at the beginning of July of this year, a number of MSN Messenger users were purported to have defected to other IM programs.

Competitors such as Microsoft, IMICI, and Odigo have also resorted to adding work-arounds to their IM programs to allow them to interact with AOL products. This tactic has proven tiresome with the fact that AOL responds by changing its IM programs with patches to counteract these work-around attempts. This is a clear message against interoperability at this time, and in this manner. In the beginnings of this tactic, AOL would send a spam message to MSN Messenger users stating that they were using unauthorized software and prompted them to download the AOL IM client. An anonymous AOL employee pointed out in a news.cnet.com article that, "You see a next-generation parallel to what Microsoft was trying to do in 1997 with the browser (Hu – "Did AOL Shoot the Messenger?")."

The FTC and the FCC was forced to face this issue when it was examining the merger of AOL and Time Warner. Through its observations and conclusions, AOL Time Warner was allowed to maintain its present non-interoperability strategy as long as it did not offer "advanced, IM based high-speed services" according to the FCC. Deborah Lathen, chief of the cable services bureau at the FCC, stated that, "AOL's

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

dominance in the instant-messaging field was based on AOL Time Warner's own innovation and marketing skills." Lathen added that the FCC has not made a determination on how to classify IM, whether it is an indispensable medium, or classifying it with the likes of say dominating long-distance telephone lines.

An interesting pressure for interoperability has come from the U.S. Navy who has begun using IM technology this year. IM is being used to debrief commanding officers of U.S. Navy battle groups according to www.thestandardc.com's article "Business Gets the Message" by Aaron Pressman. The Navy is joining many large corporations in harnessing IM application solutions that enables them to manage users and security.

In January of this year, the FCC chairman William Kennard indicated that signs like the America Online, Time Warner merger should urge policymakers to think differently in policymaking as it relates to regulating the Internet. Kennard emphasized that some of the Internet's strength lies in the fact that it is such a free and open platform, but wants to ensure that it is truly and open infrastructure.

AOL has stated that its goal is interoperability, but interrelates that there are a number of barriers to overcome before this can occur. AOL stated these reasons in a memo to the Internet Engineering Task Force in June of 2000. Rendezvous, a proposed interoperability standard, was initiated in development by AOL in 2000. However, AOL Time Warner has warned in statements that interoperability, and especially an improperly designed unified IM system, would put privacy and security at risk, as well as promote spamming and escalate other risks including hackers' ability to spam IM with pornography. This last statement in defense of the competition in the IM landscape leads us into the next topic of discovery, the potential risks to the Internet citizens who are the audience for this technology's war arena.

Issues

Although most of the media and attention in the developing area of IM has been focused on the capabilities of the IM programs, attention must also be paid to the risks that are being created or amplified because of the capabilities that IM technologies are bringing to the market.

Some of the most significant issues deal with privacy and security on this new communication channel. In news.cnet.com's article "ICQ Logs Spark Corporate Nightmare", Paul Festa reported upon a case in March of this year in which thousands of confidential messages that were sent between various CEOs and top executives were posted on the Internet. This attack was posed against the PC of Sam Cain, the CEO of eFront. The successful privacy violation was the result of ICQ's incoming/outgoing message logging capability being turned on for that program. Similarly, cnn.com reported in June of this year of two ICQ servers that were cracked resulting in Web Pages being defaced. Fortunately, the extent of the damage by this attack was minimal, yet embarrassing.

The above privacy violations come after numerous warning articles from a variety of sources warning and reminding IM users of what could and has already happened. ICQ and other IM programs state specifically on their web sites that the program should not be used for communicating sensitive information. An article back in 1998 by James Glave for www.wired.com was entitled "Net Messaging Called 'Catastrophic'" and went on to warn users of IMs inability to provide sufficient barriers against "hijacking, spoofs, and other hostile programs that can listen in on personal, and potentially sensitive, communications sent over the system." Glave described IM as writing on big cue cards in which

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

everyone can see what is being communicated. Another article (news.cnet.com – "Start-ups Strive to Lock Down IM at Work", Festa) shortly following the ICQ log copying incident underlined the risk for Executives and other employees who transfer unencrypted information over this insecure avenue.

***Figure C** to the right provides a picture of the various major entry points for intrusion within a messaging system.*

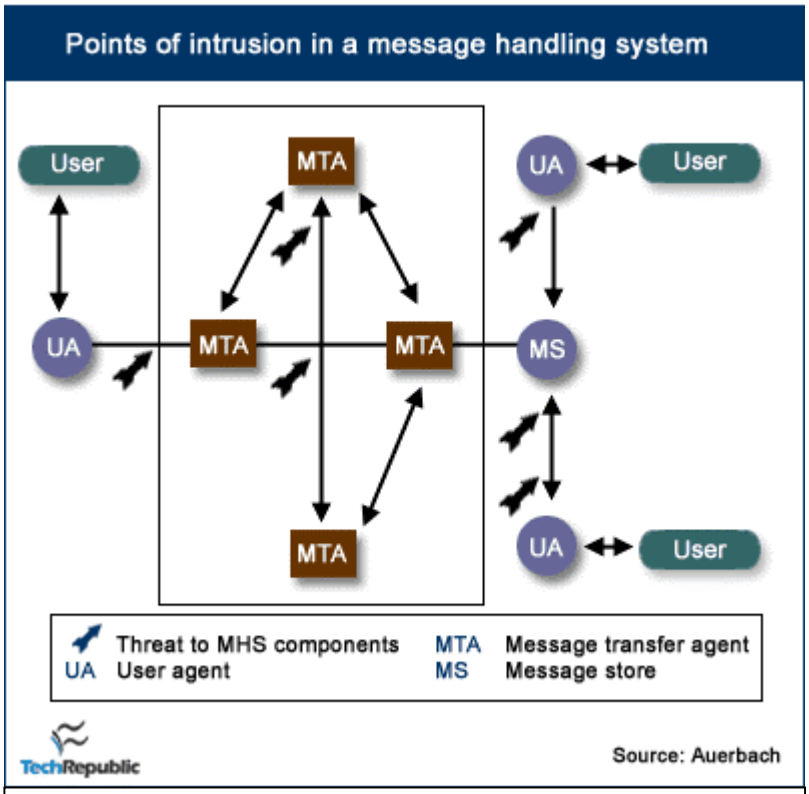

Figure C:
"Security in electronic messaging systems."
Auerbach Analysis.
21 August 2001.

In addition to privacy becoming an issue relating to IM, information security is also being threatened by malicious code that can be propagated via IM channels. Users can import viruses, export marketing intelligence, trade secrets, or harassing remarks through IM according to Howard Millman of CNet. Infected files, nuisance worms, and viruses have been slowly infiltrating the IM world according to Jim Hu of news.com who brings these realities to light in his article "Worms Find Fertile Ground in IM". One example of a worm involves a stream of "emoticons" that flood a users IM program under the guise of george.w.bush@whitehouse.gov. The worm then asks the user to accept a file (the worm) called choke.exe. The potential for this threat is only magnified by the fact that most antivirus products do not stop IM viruses.

Other concerns are mounting against the use of IM, especially in the workplace. Users and employees who use the program look to IM as being a nuisance during busy periods of time, even though one can simply disconnect or post an "Away" message. Some managers look at the technology as wasting employees' time and effort. New IM banner add advertising capabilities, AOL's instant text box advertisements, and the development of target market IM spamming are potential nuisances as well.

An article released early this month on www.wired.com was entitled "Hello AOL, I'm Listening". In the article, Leander Kahney investigated a new application of AI in the IM world. Kevin Fox hooked up an AI program named AOLiza to the AOL IM community. The program is based on an AI program Eliza that was developed by two professors at MIT in the 1960's and uses a library of stock questions to ask users questions. During its test in the IM community a number of users thought that they were talking with a real individual and answered a number of personal questions asked by AOLiza. One of the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

conversations lasted for an hour and a half. A unique fact of IM is that both users of an IM peer-to-peer link must sign-off before the link is completely severed. The capabilities for this type of technology to be harnessed by marketers, crackers, or just snoopy people would present an interesting privacy issue. Eliza type programs and "bots" could be used to initiate connections, gather and store information about users, spoof, send malicious programs to users, and keep numerous half-open sessions for later use or as a denial of service attack.

Solutions

The discussion thus far should bring an understanding of what the IM technology is, who are some of the major players in the arena, and what risks come with the added freedoms that the IM technologies have provided. With every new freedom and understanding of the risks in that environment, a new sense of responsibility must be taken upon. In this section we will see some of the strategies and solutions to help protect information assets against the risk exposure issues that have been raised.

The first step to developing a solution for protection against IM threats is to come up with a strategy. The first step of this is deciding whether you or your organization needs IM technology. This can take the form of a cost/benefit analysis based on features and/or ROI. ROI for instant messaging will be hard to determine and is likely to be ubiquitous as that of integrated messaging has been.

There are a lot of other products that meet the same needs that IM meets. For businesses, online collaboration sites such as Intranets.com, WebEx, and ScheduleOnline. These sites range from a user price of free to twenty dollars and offer encryption, password-controlled document exchange, data storage, collaboration, and embryonic project management (www.cnet.com, Millman). Microsoft's SharePoint product will be available with Office XP and offers Web and Intranet collaboration services. In order to meet the needs of instant information, Push Technologies on Web Pages like my.yahoo.com and other user specific sites can provide real updates, as well as news services available to pagers, Cellular Phones, and PDAs. Instant e-mail notification can be enabled through e-mail notification signal available in most e-mail applications, and multiple e-mail accounts can be consolidated and forwarded to a single user account. Some services are beginning to be offered to allow e-mail notification to be received via Cell Phones, and this capability can be taken so far as to allow e-mail messages to be translated into voice messages that can be retrieved via a phone.

There are still a number of IM product choices to choose from if one decides after analyzing what needs are to be met and decides that IM is the technology is best suited to meet this need. It is not the purpose of our discussion here to outline all of the available IM products. However, there are some key distinctions to keep in mind. Ezenia!, Bantu, Lotus, and Jabber cater to companies' enterprise solutions for companies. Lotus SameTime encrypts instant communications, works behind a firewall, and allows for centralized management (www.cnet.com, Millman). Jabber is flexible due to its open source developed XML base. Jabber also provides an increased amount of centralized management since it uses the standard Internet port 80 (Jabber.org). This allows network administrators to log and track messages. Microsoft's MSN Messenger integrates well with other Microsoft applications and the future for HailStorm based solutions as well as Exchange server IM capabilities offers a portfolio of solutions. The distinctions made in the competition section are important to remember. AOL's AIM and ICQ are interoperable between one another but not with any of the other competitors' applications. There is a move towards a unified standard for all of the competitors in the IMUnified collaborative composed of most of AOL's competitors. Lastly, AOL has a large percent of the IM market, some estimates have said

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

that this share of the pie is as large as eighty-percent to ninety-percent of the IM community. One may want to consider application service providers where information will be communicated to external users (www.techrepublic.com, Batchelder and Grey).

Hardware and Infrastructure considerations should also be evaluated and addressed during the selection of the product. Virus software should also be checked to ensure that the antivirus software would protect against IM traffic. If it does not, there may be a patch, new version, or other antivirus vendor to consider implementing in addition.

Another fact to consider is how many users will need to use the application if it is being considered as an enterprise solution. With this in mind, the option and customized features of the IM application can be configured to meet needs and limit risk exposure to this limited number of people. With the users and business needs defined, policies and procedures should be established for deployment, usage, and management of the selected IM product.

Once these policies and procedures have been defined, users and network administrators should go through a training exercise to familiarize themselves with the product, its functionality, and the organization's governance of its usage. Network Administrators should go through additional training in order to support the expanded centralized management role.

The next step would be to deploy an IM solution behind a firewall. The firewall should be configured appropriately to allow your solutions traffic outside, but to block incoming traffic from unsupported or unauthorized free IM services. There may also be a need for servers to be configured or reconfigured. Some solutions and recommendation involve installing a chat server separate from other servers. Jim Boyce gives a good highlight of features to configure for Exchange 2000 Server Instant Messaging in his www.techrepublic.com article on "Managing Instant Messaging Users".

Future

The future in this arena as with many of the other technology arenas shares in a bright future with expanding capabilities, movement towards standards and interoperability, consolidation of competitors, and technology convergence echoing the similar story of web-browsers during earlier stages of the Internet build-up.

The capabilities of IM are expanding in two directions, one is the various capabilities of programs themselves, and the other is the devices that will be able to use IM technology. Sun and AOL Time Warner are working on advanced instant messenger software for customers within the companies' iPlanet partnership. The program is being developed by Project RAC (Real-time Asynchronous Communications) (www.zdnet.com, Shankland). The software's capabilities are said to include broadcast messaging, channel subscription, ability to poll groups on questions, chat rooms, forwarding messages to cell-phones, and centralized user information. AOL has been pursuing whiteboard, telephony, video, PC-to-Phone, and cell-phone capabilities for its future product releases. AOL has been working with GSM (Global System for Mobile communications), SMSs (short message service – a basic GSM utility), SMSCs (Short Message Service Centers - a clearinghouse for text messages), and GPRS (General Packet Radio Service – allows users to stay logged on AIM for indefinite periods of time for less money) (www2.infoworld.com, Sayer).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Microsoft is scheduled to release an upgraded version of its Windows Messaging software on Oct. 25 along with Windows XP (www.zdnet.com, Shankland). Microsoft's development blocks under the name HailStorm will work in concert with all applications, with the Windows OS, with new versions and support from Hotmail, MSN Messenger, and Passport authentication. HailStorm's goals are to popularize and draw support for the .Net services, making it more popular to third-parties and increasing loyalty to Microsoft and its subscription-fee based strategy (www.news.cnet.com, Wilcox).

Jabber.org is working with Nuance to develop speech recognition services. Odigo is cooperating with Audium for voice access to IM applications. Activebuddy's search client was recently released allowing users to submit queries (www.zdnet.com, Festa). Yahoo and Microsoft are working with technologies to pinpoint the location of wireless devices for expanded IM capabilities. Yahoo's messenger now alerts user to information about new e-mails, stock prices, and auction activity. AOL, Yahoo, and Microsoft have enabled IM programs to offer free long-distance Internet phone calls (www.freep.com, Fortt).

Recent progress has been made in the interoperability battle. AOL Time Warner had to give a progress report to federal regulators late July. Within this meeting, AOL communicated that it plans to test its AIM product with other IM products using one of the proposed standard IM technologies.

The battles portrayed here describe those that have raged between companies, standards, regulating bodies, competing technological ideas, users, and service providers. The victories in these battles determine the future means in which information will be communicated, and finally, how secure the contents of these communications may be in the future - but the war is not over.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Batchelder, Robert et al. "Commentary: Free IM-not to be trusted." Gartner. 12 July 2001. URL:http://www.techrepublic.com/article.jhtml?src=search&id=r00120010712ggp01.htm (12 September 2001).

2. Boyce, Jim. "Managing instant messaging users." 16 October 2001. URL:http://www.techrepublic.com/article.jhtml?src=search&id=t01320011016boy01.htm (12 September 2001).

3. Dean, Katie. "Instant Messaging Grows Up." 25 January 2001. URL:http://www.wired.com/news/print/0,1294,33736,00.html (12 September 2001).

4. Disabatino, Jennifer. "Hackers penetrate ICQ instant message servers." June 28, 2001. URL:http://www.cnn.com/2001/TECH/internet/06/28/hackers.penetrate.aol.idg/index.html (11 September 2001).

5. Festa, Paul. "ICQ logs spark corporate nightmare." 15 March 2001. URL:http://news.cnet.com/news/0-1005-202-5148422.html (11 September 2001).

6. Festa, Paul. "Pushing the envelope on IM." 30 July 2001 URL:http://www.zdnet.com/filters/printerfriendly/0,6061,5094919-2,00.html (12 September 2001).

7. Festa, Paul. "Start-ups strive to lock down IM at work." 26 April 2001. URL:http://news.cnet.com/news/0-1005-202-5729145.html (11 September 2001).

8. Foley, Mary Jo. "Microsoft readies HailStorm against AOL." 15 Febraury 2001. URL:http://news.cnet.com/news/0-1003-202-4825884-0.html (12 September 2001).

9. Fortt, Jon. "Instant message is the medium." AOL keeps Software other companies covet. 16 Janauary 2001. URL:http://www.freep.com/money/business/mess16_20010116.htm (12 September 2001).

10. George, Tischelle. "Alaska Airlines Adds Instant Messaging To Customer Service." 24 April 2001. URL:http://www.informationweek.com/shared/printableArticle?doc_id=IWK20010424S0009 (12 September 2001).

11. Glave, James. "Net Messaging Called 'Catastrophic'." 5 June 2001. URL:http://www.wired.com/news/print/0,1294,12758,00.html (12 September 2001).

12. Goodin, Dan. "Instant Messaging's War of Words." The Industry Standard Magazine. 10 January 2001. URL:http://www.thestandard.com/article/0,1902,8465,00.html?printer_friendly= (12 September 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

13. Harmon, Kyle. "Instant message options for the corporate environment." 3 February 2000. URL:http://www.techrepublic.com/article.jhtml?src=search&id=r00320000203hrm10.htm (12 September 2001).

14. Helft, Miguel. "Talking the Talk across the Net." 19 June 1997. URL:http://www.wired.com/news/print/0,1294,4525,00.html (12 September 2001).

15. Hu, Jim. "AOL must move to share IM." 23 July 2001. URL:http://www.zdnet.com/filters/printerfriendly/0,6061,5094503-2,00.html (12 September 2001).

16. Hu, Jim."Did AOL shoot the messenger." 5 April 2001. URL:http://news.cnet.com/news/0-1005-202-5464191-0.html (11 September 2001).

17. Hu, Jim. "Worms find fertile ground in IM." 14 August 2001. URL:http://www.zdnet.com/filters/printerfriendly/0,6061,5095671-2,00.html (12 September 2001).

18. Kahney, Leander. "Hello AOL, I'm Listening." 1 September 2001. URL:http://www.wired.com/news/print/0,1294,38517,00.html (12 September 2001).

19. Manjoo, Farhad. "Instant Message Still AOL's Deal." 13 January 2001. URL:http://www.wired.com/news/business/0,1367,41161,00.html (12 September 2001).

20. Millman, Howard. "Instant messaging equals instant trouble." Cnet.com. 29 August 2001. URL:http://www.techrepublic.com/article.jhtml?src=search&id=r00220010829cnt01.htm (12 September 2001).

21. Oakes, Chris. "Upstart Says Hello to AOL's ICQ." 24 January 2001. URL:http://www.wired.com/news/print/0,1294,33882,00.html (12 September 2001).

22. Olsen, Stefanie. "IM buddy making more powerful friends." 23 May 2001. URL:http://news.cnet.com/news/0-1005-202-6021116.html (12 September 2001).

23. Pressman, Aaron. "Business Gets the Message." The Industry Standard Magazine. 26 February 2001. URL:http://www.thestandard.com/article/0,1902,22221,00.html?printer_friendly= (12 September 2001).

24. Pressman, Aaron. "Kennard's Instant Message." The Industry Standard Magazine. 22 January 2001. URL:http://www.thestandard.com/article/0,1902,21459,00.html?printer_friendly= (12 September 2001).

25. Sayer, Peter. "AOL buddies with mobile phone users via short message service." 22 February 2001.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

URL:http://www2.infoworld.com/articles/hn/xml/01/02/22/010222hnaolgsm.xml?Template=/storypages/printfriendly.html (12 September 2001).

26. Shankland, Stephen. "Sun, AOL partner on corporate IM. " News.com. 16 July 2001. URL:http://www.zdnet.com/filters/printerfriendly/0,6061,2787072-2,00.html (12 September 2001).

27. Vance, Ashlee. "Microsoft, Yahoo, others set to link IM services" 8 February 2001. URL:http://www2.infoworld.com/articles/hn/xml/01/02/08/010208hnim.xml?Template=/storypages/printfriendly.html (12 September 2001).

28. Wilcox, Joe. "Microsoft's HailStorm unleashed." 19 March 2001. URL:http://news.cnet.com/news/0-1003-202-5181485.html (12 September 2001).

29. *None*. "File Trading Takes AIM at AOL." Wired News Report. 8 August 2001. URL:http://www.wired.com/news/print/0,1294,38118,00.html (12 September 2001).

30. *None*. "ICQ Inc. - Contact Us." URL:http://www.icq.com/company/about.html (11 September 2001).

Images:

Figure A. Tech Republic. "Most organizations aren't using IM." 12 June 2001. URL:http://www.techrepublic.com/article.jhtml?src=search&id=r00120010612sta01.htm (12 September 2001).

Figure B. URL:http://www.thestandard.com/img/body/9619.gif – Work vs. Home. (12 September 2001)

- Pressman, Aaron. "Business Gets the Message." The Industry Standard Magazine. 26 February 2001. URL:http://www.thestandard.com/article/0,1902,22221,00.html (12 September 2001).

Figure C. *None*. "Security in electronic messaging systems." Auerbach Analysis. 21 August 2001. URL:http://www.techrepublic.com/article.jhtml?src=search&id=r00520010821aue01.htm (12 September 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced