Global Information Assurance Certification Paper

Charles Amman
GSEC Practical Assignment V. 1.4b Option 1
August 5, 2004

Real time messaging programs:
An unavoidable reality on today's business networks; can be a useful tool when implemented with appropriate safeguards in place.

Abstract

Public chat software such as AOL instant messenger has not always been a welcome application on business networks. Despite the fact that they are riddled with security and administrative shortcomings, publicly available instant messaging software usage has grown due to grass roots implementation in the workplace. As businesses come around to the productivity potential of instant messenger applications the state of the technology struggles to answer the demands for secure, accountable, and interoperable solutions. At this time the demands have been met by a combination of the efforts of instant message network operators and third party solution providers. The question that remains is will businesses adopt these solutions? Will businesses continue to tolerate these unsecure and exploitable programs on their networks or will they reject the potential of instant messaging altogether?

Backgorund

Since their introduction real time messaging programs in the business environment have been considered taboo for a number of reasons. Security professionals despise them for being vulnerable security holes; Managers view them as productivity drain and a distraction for their employees. However, more and more they are being incorporated into the business environment as an inexpensive and convenient tool for team communication. In this paper I will explore the historical pitfalls of the AOL Instant Messenger program and the recent technology advancements that have been made in an effort to make this and other public chat programs more viable applications on the secure business network.

AOL instant messenger grew out of the popularity of the chat features of America on Line's subscription service. A free stand-alone application, users who already have a connection to the internet can install the AIM application, register a screen name with AOL, and send instant messages to any of AOL's reported 200 million registered users. In addition to short text messages, also known as instant messages, AOL and its competitors continue to add other features which include file transfer, video and audio communication. Many people have discovered the ease and convenience of communicating via instant message, and unauthorized ad hoc instant messenger networks have popped up on many business networks. The use of AIM and other public instant messenger products

is not without controversy. Instant messenger can be a powerful tool for business collaboration via its ability to enable real time communication between coworkers, but it can also be an unregulated distraction used for personal conversations.

The Gartner group has projected that up to 70 percent of corporate networks now utilize public instant messenger applications and IDC estimated that up to 29% of the traffic on these public chat networks is attributable to business usage.[1] AOL estimates these numbers to be even higher, with 84% of enterprises having some type of instant messaging either officially or unofficially deployed on their networks.[2] Whatever the number is, instant messaging has a foothold in the corporate environment and should not be overlooked. The advocates of instant messaging technology in the workplace have sited many examples of increased productivity, or efficiency at resolving problems. In an associated press article published in the USAToday on August 4th 2003, the author describes the implementation of an AOL based corporate messaging product at the Carl's Jr. headquarters which dramatically improved help desk response time resulting in improved customer service.[3] Additionally an AOL sponsored workplace study demonstrated that the use of instant messenger has the potential to improve productivity in "workgroups where high availability and speed of response were highly valued, such as sales and customer service."[4] The study also pointed out that the use of Instant messenger can be particularly useful for backchannel discussions during telephone conference calls and similar scenarios.

Despite the usefulness of AIM there are multiple security complaints that have been lodged against this technology. The lack of message text encryption, insufficient identity assurance of the person sending the message, and the file transfer feature which allows for the transfer of files that evades virus detection programs. In addition to those security concerns there are administrative deficiencies due to the ad hoc nature in which these programs are deployed. The lack of a centralized way to log and monitor conversations is a major concern for managers who would like archive conversations and monitor them for inappropriate content. Additionally the inability to easily allow or disallow instant messenger usage for individual users on the network has left administrators impotent to offer the fine level of permissioning that managers have come to expect.

Instant Messaging Vulnerabilities

The primary security flaw of AIM is that messages are sent in clear text. What is equally alarming is the fact that most end users do not realize that this is the case. Combine these two factors and the result is the possibility of unknowingly

[1] Sarrel
[2] AOL Messaging solutions – Instnat Messaging for Enterprises.
[3] Associate Press article, 04 Aug 2004
[4] AOL Messaging solutions – Effects of Instant messaging on Enterprise Performance

transferring sensitive personal information or proprietary business data directly into the hands of someone who intends to misuse it. This contention may be blown a bit out of proportion since, given the large volume of data that would have to be sifted through and the fact that a network sniffer would need to be set up on the network in order to eves drop, the chances of this actually happening is probably low. However, the threat is a real possibility, and has caused many managers and computer security professionals to take notice of this serious security flaw.

User identity assurance is another problem for corporate users. The fact that these public IM networks are not administered by the corporations that use them means that naming conventions are not always followed. Furthermore, the AIM password policy only requires a minimum of a four characters, with no requirement for special characters, capitals or numbers. Additionally, since passwords never expire, the AIM policy is a far cry from what even the most relaxed corporate password policy would allow.

A handy addition to the AIM feature set, the file transfer function allows for the transfer of any type of file to another AIM user. By importing a file in this matter, the AIM user exposes his computer and corporate network to the possibility that the transferred file contains a virus, or worm since this method evades traditional safeguards such as email filters or virus scanning software.

The lack of any convenient archiving feature in AIM means that a record of what was discussed during a chat session is not available once a chat session has been ended. For this technology to even be considered by businesses which requires electronic communications archiving, a centralized depository that allows for easily searching messages must be implemented. As Sarrell stated in his November 2003 column in PC magazine, the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability act of 1996, the recently updated SEC Rule 17a-4 and the subsequent National Association of Securities Dealers notice to members, all consider corporate instant messages equivalent to email and subjects them to the same rules governing the handling of corporate email messages.

Many managers are uncomfortable with the fact that IM conversations cannot be monitored for content. The fact that instant messenger applications can very easily be abused by using them for personal conversations has led prudent managers to avoid approving its use. Without the ability to monitor activity a business does not know if they are opening themselves up to legal issues resulting from inappropriate communications, the transmission of pornographic or copyrighted material. Furthermore, outbound file transfers pose a corporate espionage risk in that they enable an employee to export files out of the business network without the traditional audit trail that might leave traces of such activity.

Remedies

The security risks posed by Instant messenger software have become a serious concern for network security professionals. Historically companies have dealt with this nuisance by simply blocking instant messenger traffic on their firewall. At first this was as easy as blocking port 5190, but as AIM matured it was programmed to find ways around firewalls. AIM accomplished this by choosing other ports to communicate on including such common ports as 23, 80 and 113. Obviously outbound traffic on the ports used for telnet, http and tcp could not be blocked, so other solutions were necessary such as blocking traffic to the AOL authentication servers.

In response to the need to make their AIM software more secure AOL incrementally began to address some of the concerns by adding an encryption feature that enable end-to-end encrypted communication in AIM 5.2 and in version 5.5 they added local virus scanning for transferred documents. For most companies, these efforts did not go far enough to remediate corporate concerns. In the summer of 2003 AOL released the AIM Enterprise Gateway server, which was designed to address a majority of the AIM security deficiencies about which businesses were complaining.

In the release of AIM 5.2 AOL partnered with Verisign to provide a public key encryption solution to secure IM, chat and file transfer traffic. This feature allowed for end to end encryption of messages which digitally signed the communications being sent. By employing this technology, recipients and senders have the assurance from Verisign that their communication could not be read by unauthorized third parties, and that the communication had not been altered while in transit. One important excepteion to note is that users on networks which employ AOL's AIM Enterprise Gateway server, which I will discuss shortly, do not enjoy complete protection while engaging in encrypted communications. The AIM Enterprise Gateway server has the ability to decode encrypted messages as part of its logging and monitoring functions.

The Verisign Public Key Infrastructure works by assigning users a public and a private key. The public key is readily made available through the AIM network, however the private key is meant to be kept secret and is never shared. When encrypted communications are to be sent, the recipient's public key is retrieved by the AIM progam and is used to encode the message. This encoded message is then sent over the network to its intended recipient. Once the recipient receives the message their AIM program uses their own private key to decode it. If the message were intercepted by an unintended third party the information they would see would be an unintelligible array of symbols and numbers. The security of this type of communication is ensured because the holder of the private key that corresponds to the public key which encrypted message is the only one who is capable of opening the message. For this reason it is vital that the private key remain secret.

With the release of AIM 5.5, AOL added a virus scanning feature which, when turned on, would automatically check all transferred files for viruses. To many home users this and the ability to encrypt communications were welcome additions to the AIM software, however for most corporations they didn't go far enough. In the case of encryption they solved one problem but created another one by making it even harder for companies to monitor and log messages since the intercepted encrypted data was unintelligible and could only be unencrypted with the recipient's private key or by using the AIM Enterprise Gateway server.

Developed in partnership with FaceTime corporation AOL launched its AIM Enterprise Gateway server. AOL's first product aimed at the business environment, it contained much of the functionality that businesses and security professionals were asking for. The capabilities of the gateway server include encryption key management, message logging, message monitoring, virus scanning, identity management and reflection of internal messages.

The AIM Enterprise Gateway server was designed to be a central point where all instant message traffic on a network would be converged and processed before being allowed to travel outside the corporate network. The logging and monitoring of encrypted messages was made possible by giving the gateway server the ability to decode those messages before entering them into its database. Identity management is accomplished by support of LDAP integration with enterprise authentication systems such as Active Directory. The AIM Enterprise Gateway server also affords the administrator the ability to construct custom reports on IM usage, and search for keywords and phrases within IM conversations. Lastly, the gateway server serves as a central checkpoint for scanning of incoming files for viruses and worms.

Third Party Corporate Solutions

In June of 2004, AOL announced that it would discontinue its AIM Enterprise Gateway server product, following Yahoo's lead a week earlier which also discontinued its Business Messenger product. AOL explained this move similarly to Yahoo by saying that had not lost interest in the corporate market, but that it was no longer going to pursue development of the software needed by business clients. [5] AOL assured its continued involvement in the business market through its partnerships with third party companies such as IM Logic, FaceTime (which developed AIM Enterprise Gateway for AOL), and Akonix Systems.

Many third party solution developers have emerged on the market with products aimed at remedying the security and administration flaws of publicly available chat products as well as others who circumvented these problems by providing proprietary internal instant message solutions. FaceTime, IM Logic and Akonix are three companies which have parternered with AOL to provide AIM based solutions for corporate clients. In a similar way these companies have all

[5] Perez

addressed many of the concerns that businesses have regarding public chat software while retaining the usability and productivity features that the end user has come to rely on.

The IMlogic product was chosen by AOL to be the successor of the AIM Enterprise Gateway server. The IM Logic product consists of two components: the IM Manger, and the IM Linkage. IM Manager incorporates and improves upon all of the elements that were part of the AIM Enterprise Gateway server and adds a number of additional administration and security features. IM Linkage adds protocol translation functionality, allowing users on different instant message networks to interoperate.

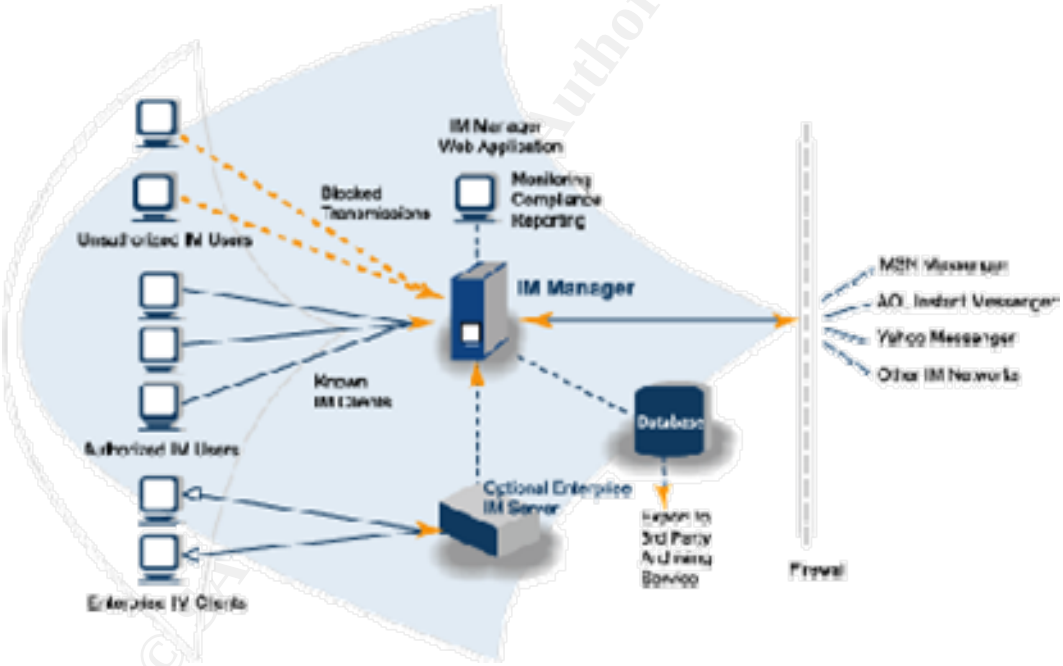
The IM Manager employs a proxy-like architecture similar to that of the AIM Enterprise Gateway. Improvements include the use of multiple virus scan engines to screen incoming files, and content filtering that allows key-word and phrase-blocking in instant messages. The ability to control who in the enterprise can use Instant Messenger products is greatly improved with the IM logic product. Permission features are provided as an extension of existing enterprise authentication systems such as Active Directory which are tied into IM Logic controls via an LDAP connection. The finer permissioning capabilities allow the administrator the ability to set file transfer permissions based on user and by specific files thereby controlling the traversal of sensitive documents within the business network. Administrators are also able to restrict internal and external IM usage granularly by specifying recipient screen names on the IM Manager server, therefore preserving the productivity advantages of sending instant messages outside the corporate network while at the same time controlling abuse by being able to effectively restrict personal conversations.

Additionally, IM Manager has incorporated a feature that keeps track of client software versions. Version control helps network administrators know which versions of the AIM chat software are in use on their network, and allows him to set restrictions based on version including patch level status. The acceptable versions may be chosen based on necessary features, known security vulnerabilities or other criteria set by management. Additionally a SPIM control component has been incorporated into the IM Manager product. SPIM is the instant message equivalent of email SPAM, which is classified as unsolicited commercial messages sent over instant message networks which are usually sent out using automated technology. These SPIM messages are automatically identified and blocked from entering the network by IM Manager as a way to limit the disruption of workflow and eliminate the potential that inappropriate material, or links to malicious content enters the environment.

A powerful addition to IM Logic's software solutions, IM Linkage addresses one of the biggest pitfalls of existing public chat software. IM Logic has incorporated a protocol translation feature into IM Linkage which allows for interoperability between 12 of the most popular chat clients. The added convenience of

interoperability reduces previous migration roadblocks by allowing existing heterogeneous ad hoc instant messenger networks to be incorporated into the official enterprise solution. The chat clients which have been incorporated into the protocol translation feature include the usual publicly available networks such as AOL, Yahoo, and MSN, as well as some of the more common business messaging solutions such as Microsoft Office System Live Communications Server 3003, Microsoft Exchange 2000, IBM Lotus Instant messaging (formerly Sametime) and Yahoo Business Messenger. Other less common messaging clients that also interoperate with IM Linkage include: Jabber, Anteopo, Reuters Messaging, Hub IM, Bloomberg IM, and Parlano Mindalign IM messages. Integrating, existing public chat software, business grade solutions as well as proprietary internal chat clients into IM Manager with IM Linkage serves to improve the state of instant message security by allowing for centralized control, and the centralized administration of security features such as encryption and identity accountability.

The following graphic illustrates the components of the IM Manager system and the flow of instant message data on a typical business network.



6

Conclusion:

AOL Instant Messenger and other consumer-grade instant message software are unavoidable entities on many corporate networks. This mode of communication is rapidly becoming an accepted and sometimes preferred method of communication within the corporate environment. Not initially intended for

[6] Figure source: http://www.imlogic.com/solutions_imm.htm

corporate use, network administrators and security professionals are challenged with the task of providing accountability and security to this type of communication. The leaders of organizations must work with IT staff to understand the advantages, and limitations of this type of software and work to establish policy which best fits their organization. If they choose to embrace instant messenger they must invest in technology designed to safeguard IM communications itself, as well as safeguard their other network investments from the vulnerabilities that IM applications could open expose them to.

Banning IM in your organization may be the answer; educating your users about appropriate use and the risks that are associated with public chat technology may work for an organization with a limited budget; or implementing an enterprise IM management solution may be the most economical way to mitigate risk but still give employees the tools necessary to do their job.

References

AOL Messaging Solutions “Effects of Instant Messaging on Enterprise Performance, Results of a Longitudinal Study.” URL: http://www.aimatwork.com/whitepapers/RIM_ROI-full_wp.pdf (04 Aug 2004)

AOL Messaging Solutions “ Instant Messaging for Enterprises – How it works, Key Benefits and Enterprise Requirements URL: http://www.aimatwork.com/whitepapers/IMbenefits-wp.pdf (04 Aug 2004)

Associated Press “Instant messengers take corporate world by storm” 04 Aug 2003 URL: http://www.usatoday.com/tech/news/techinnovations/2003-08-04-im-at-work_x.htm (04 Aug 2004)

Bird, Drew “Instant Messaging: Corporate Productivity Tool or Cool toy?” 01 May 2003 URL: http://www.intranetjournal.com/articles/200305/pij_05_01_03a.html (04 Aug 2003)

Clyman, John “AIM Enterprise Gateway 2.0” 11 Nov 2003 URL: http://www.pcmag.com/article2/0,1759,1357964,00.asp (29 Jul 2004)

Hu, Jim “New AOL IM program offers encryption” 30 June 2003URL: http://news.com.com/New+AOL+IM+program+offers+encryption/2100-1032_3-1022269.html (04 Aug 2004)

McEachern, Cristina “e-mail alert” 16 Jul 2002 URL: http://www.financetech.com/story/featured/showArticle.jhtml?articleID=14702745&pgno=2 (04 Aug 2004)

Oldversion.com “AOL Instant Messenger” URL: http://www.oldversion.com/program.php?n=aim (04 Aug 2004)

Pruitt, Scarlet “AOL Adds IM Encryption” 30 June 2003 URL: http://news.com.com/New+AOL+IM+program+offers+encryption/2100-1032_3-1022269.html (04 Aug 2004)

Pruitt, Scarlet “AOL Moves Messaging to Buisness: 4 Nov 2002 URL: http://www.pcworld.com/news/article/0,aid,106608,00.asp (04 Aug 2004)

Perez, Juan Carlos “AOL Phases Out Business IM” 21 June 2004 URL: http://www.pcworld.com/news/article/0,aid,116603,00.asp (29 July 2004)

Pruitt, Scarlet “IMlogic Boosts IM Security” 12 April 2003 URL: http://www.pcworld.com/news/article/0,aid,110259,00.asp (04 Aug 2004)

Sarrel, Matthew D. “Corporate IM” 11 Nov 2003 URL: http://www.pcmag.com/article2/0,1759,1359496,00.asp (29 Jul 2004)

Tschabitzcher, Heinz “AOL Instant Messenger 5.5” URL: http://email.about.com/cs/windowsimclients/gr/aol_instant_msg.htm (04 Aug 2004)

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS