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.

Understanding Instant Messaging (IM) and its security risks

Instant messaging is very popular in consumer sector. However, it has yet to be used widely in the commercial sector as e-mail is currently used. The major drawback has been the vulnerabilities associated with IM technology. These vulnerabilities have created several security issues. The security issues have made organizations think before exploiting IM technology. This paper provides an overview of IM technology. It discusses vulnerabilities of IM and related security issues. This paper also provides an insight in to ...

Copyright SANS Institute
Author Retains Full Rights

AD

Sujata Chavan
Date of submission – August 25th, 2003
GIAC Security Essentials (GSEC) Certification Practical Assignment
Version 1.4b – Option 1

Understanding Instant Messaging (IM) and its security risks

Abstract:

Instant messaging is very popular in consumer sector. However, it has yet to be used widely in the commercial sector as e-mail is currently used. The major drawback has been the vulnerabilities associated with IM technology. These vulnerabilities have created several security issues. The security issues have made organizations think before exploiting IM technology. This paper provides an overview of IM technology. It discusses vulnerabilities of IM and related security issues. This paper also provides an insight in to the considerations an enterprise should give during the implementation of IM technology and related products.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Understanding Instant Messaging (IM) and its security risks

In May 2003, Yahoo Instant Messaging (IM) and the combination of Web Camera was my savior. I had surgery that affected my voice, which in turn prevented me from conversing on the phone. I knew this was going to be emotionally very hard on my family abroad who could not hear my voice. But with the latest technology in Instant messaging area we mitigated this tense situation. Day after my surgery, from the comforts of my home, I just hopped on Yahoo Instant Messenger. My family could see me in person on Web Cam. They could not hear my voice but my well being was communicated to them via Web camera. My father thanks the Web camera and tells me how relieved he felt just to be able to see me online. Seeing my movements on web camera assured my family of my well being. Such effective communication and it cost me very little to make it possible.

I. Emergence of IM

In last few years Internet has set the direction of how, where and the way we communicate. E-mail has become a mainstream form of communication and has replaced the traditional letters, especially for people who live away from their families half way across the world! Who wants to wait 7 to 8 days just to know your families well being! Who wants to spend hundreds of dollars and deal with the bad connection over the telephone! Countless e-mail messages are sent and received all over the world on a daily basis.

In last couple of decades people have started using Internet regularly. The need of live and sensible way of communication over Internet has increased rapidly. The start of Instant Messaging came about in 1996. Instant Messenger is client software that allows person to person interactive communication in real-time provided both users have the same software. Such communication is called 'chat'. Company named Mirablis, Ltd., introduced ICQ, instant messaging utility. ICQ, in shorthand language is "I seek you"[1].

II. How does IM work

Instant messaging works as its name. It delivers the user's message to his desired contact instantly. The message delivery is instant provided users contact person is online. The client software allows user to maintain a list of contacts that he wants to communicate. User can send messages to any of the contacts in his list. Such list is referred to as a buddy list or contact list. This contact list is nothing but e-mail ID of a contact. The user and his contact can send instant messages to each other provided both of them are on each other's contact list. The contact list can be managed by adding, deleting or editing the contacts e-

[1] Bird, Drew. "Instant Messaging: Corporate Productivity Tool or Cool Toy? ". Intranet Journal, May 1, 2003.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

mail ID and other related information. Also a group can be formed of different ID. Creating groups helps when sending mass communications. User can also block a particular contact or every one who is not on his contact list from sending an instant message. Setting the appropriate privacy settings does this.

When user tries to send a message to his contact the software opens up a small interactive window. In this window user and his contact can type a message. The user and his contact can see the message window and messages within the window. Messages can be printed, saved and archived. Along with text messages, a file, graphics, image or voice can also be sent instantly using the messaging.

Nowadays use of web camera makes this interaction even more thrilling. It is amazing to see the reaction of the user at the other end as he reads the instant message.

On Yahoo Messenger service user can send an offline message to the other user on the list. When the other user logs on his Yahoo Messenger, message window pops up and makes user aware of the offline message. User then can click on the offline message to read the message. This makes it much more convenient than e-mail. Microsoft's MSN Service does not provide offline message feature. If user whom you want to send message is not online then whatever message you want to send needs to be sent in e-mail format.

When user logs on Instant messenger service he can see the presence of the friends on his contact list and vice versa. User can show his availability via Instant Messenger. Sometimes user is online but is busy and do not wish to respond to any instant messages. In such situations user can change his status to 'Busy' or 'Not available'. This allows the person who is trying to contact user know the reasoning behind the non-availability of user. User can also choose to be invisible while being online. This enables him to watch his contacts without giving his status.

Various communication means are available using instant messaging. User can have an individual chat session or have a conference with multiple users. With use of web camera and voice an interactive web conference can be held using instant messaging.

III. IM Service providers/Vendors

Among the various vendors for instant messaging, America online (AOL), Yahoo and Microsoft are some of the major vendors in providing instant messaging for consumers, with AOL in the lead.

AOL Instant Messenger (AIM) – AOL has 35 million members worldwide. AIM delivers over 1.38 billion instant messages daily across the AOL network. AOL is

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

considered to have most of the IM Market share due to its vast online user base. AIM client is provided via download, to any of its customers[2].

MSN Messenger – MSN has about 9 million subscriptions. Besides the subscribers, MSN Messenger can be downloaded free of charge by anyone with an access to Internet[3].

Yahoo Instant Messenger – Just like MSN, Yahoo provides the Messenger services free of charge to anyone who wants it. Simply go to their web site and download the Yahoo Messenger. Both Yahoo and MSN support instant text and voice messages, communication face-to-face via web cameras, and affordable PC-to-phone calls anywhere in the world. Users have sent approximately 17 billion messages in December 2002 alone. In 2002, Yahoo took the IM sensation mobile through an agreement with AT&T Wireless, which lets AT&T customers and Yahoo! Messenger desktop users initiate an instant two-way chat[4].

IV. Vulnerabilities of IM

IM as a new technology has a lot of potential. Then why IM is not used by every organization? IM seems like the solution for lot of business issues. Unfortunately IM technology has quite a few vulnerabilities. These vulnerabilities directly or indirectly create security threats and thus create a potential security risk.

- IM in consumer world utilizes public networks and uses the IM provider's servers. It is referred to as public IM or external IM. These servers are not secured by any firewalls. On the other hand IM in the private network also called as private or internal IM can be secured by firewall.
- Sensitive information exchanged during an IM session is often stored in unsecured systems. As mentioned earlier Public IM provider's servers are not protected by any firewalls. It is very easy for someone to eavesdrop on IM user's private conversation.
- E-mail has become an integral part of corporate world. In large corporations e-mail is a way of mass communication. To avoid Spam and viruses entering corporate networks companies diligently filter e-mails passing through their network. Anti-virus software is used to catch any virus on the corporate e-mail system. On the other hand, files sent via IM do not pass through the corporate E-mail system. Therefore these files cannot be scanned for viruses. Computer viruses and worms can be sent through these files[5].
- Lack of encryption on Public IM network means that the IM session conducted using public network is like an open book to the entire Internet

[2] Data points. AOL: the worlds leading interactive service. Who We Are.
[3] Microsoft, Press Pass. MSN 8 Butterfly Squad Nationwide Tour Takes Flight . Feb 13, 2003.
[4] "Relating in real time". Yahoo! 2002 Annual report.
[5] Hallett, Tony. "IM creates 'rampant security risk'". ZDNet UK. February 5, 2003.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

community. Trade secrets if communicated over Public IM can become public knowledge in seconds.
- Communication via IM cannot be monitored or logged in order to maintain corporate security.

These vulnerabilities of IM pose a serious security risk to the IM users.

V. IM related issues faced by corporations

After looking at the various IM vulnerabilities one gets an idea of some of the IM related issues. Corporate world has to face these issues if IM technology is to be utilized widely.

- ***Popularity of IM*** - Popularity of IM in itself is a problem for corporations. According to Gartner, Inc. "Instant messaging (IM) services are being implemented rapidly by employees, but enterprises will be facing severe security risks"[6]. People, who are used to keeping in touch with their loved ones via IM, see nothing wrong to download the free Public IM on their work computer. Such an unauthorized installation and usage of IM is like punching a whole in corporation's Firewall[7].

- ***Legal Compliance*** – There are quite a few laws that require to protect the privacy of an individual and also maintain the proper records that can maintain the trail of individual transactions. HIPPA (Health Information Portability and Accountability Act) and Privacy Act are the recent examples. Financial institutions require that a proper log be kept of all the related account activities. Insecure IM sessions, unauthorized use of IM, lack of log records and monitoring of IM sessions etc. translates into lack of such required procedures. This could result in a lawsuit against the organization that fails to maintain such procedures. IM being so new lacks the infrastructure to maintain and create such procedures. Enterprises have to be innovative and make sure that legal requirements are satisfied. All this could mean escalated cost to use IM.

- ***Copyright*** –Potential of employees swapping copyrighted material over employer's IM network exposes the employer to copyright related lawsuits or fines. It is so easy for employees to download the copyrighted materials such as music from the Internet and then turn around and send the same file to a friend over IM.

---

[6] Gartner Press Room. Press release "Gartner Says Free Instant Messaging will be Found in 70 Percent of Enterprises within Two Years". October 2001.
[7] Vijayan, Jaikumar. "Users, Experts: IM poses Security Risk". COMPUTERWORLD. December 3, 2001.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- ***Insecure Communication*** - Businesses are required to protect information related to their customers, vendors and their own trade secret. Several specific issues come up with insecure communications in commercial sector.

  1. *Identity Theft* – This is a technological nightmare for an individual who has to live it. In identity theft an individual's identity is stolen and is used by an identity thief to conduct various monetary transactions. The person who's identity has been stolen is not aware of these transactions. By the time an individual becomes aware of such theft bad record in the system is already established. Such crime can be easily committed. Confidential information such as your bank account number, social security number, credit card information should not be shared during IM session[1].

     In Asia most of the big cities have Cyber Cafes which offer computers for hire. One observation that I have made during my use of cyber cafe is that most of the users do not realize how important it is to log out after using the service. This happens due to ignorance of the user. If you are conducting an IM session with such an ignorant user it is easy for someone to gain control of the same machine after the user has left the cafe, pose as the 'Ignorant User' and get some related important information out of you. In situations like this even the secure authentication system will fail. The imposter is taking the official charge of the account. Enterprises have to give serious thought to identity theft and its consequences. They have to take measure to protect the identity of their IM users.

  2. *Cyber stalking* - Crime such as Cyber stalking is becoming very common. In this case stalker stalks a victim on Internet. Use of E-mail or other forms of electronic communication is used by stalker as means of stalking. Presence is the most popular feature of IM. IM gives away the presence of user. This makes it easier to stalk the person online. This could mean an enterprise has to deal with the loss of employee productive hours. Measures need to be taken to hide the identity of victim from a cyber stalker. This could mean that employer will have to get involved in possible lawsuit.

- ***Immaturity*** – "The rapid proliferation of IM use has resulted in individuals employing a vital communication medium without forethought," said David Smith, vice president and Research Director for Gartner[6]. This is so true. E-mail has evolved over last 2 decades and is much more secure now. Especially with the use of modern encryption technology. The drawbacks of

---

[1] Bird, Drew. "Instant Messaging: Corporate Productivity Tool or Cool Toy? ". Intranet Journal, May 1, 2003.

[6] Gartner Press Room. Press release "Gartner Says Free Instant Messaging will be Found in 70 Percent of Enterprises within Two Years". October 2001.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IM need to be recognized and dealt with by enterprises. Considering the limitations of IM the proper security planning needs to be done.

VI. Evaluation of IM technology by an enterprise

After looking at the IM history, vulnerabilities of IM and IM related issues one thing is clear that Instant Messaging technology is here to stay. Then how can an enterprise get ready to adopt this technology? In spite of all the security risks there are quite a few businesses that currently use IM. May be because most of such business owners are 20 something who recognize the potential of IM and are willing to take risk to get ahead in the business. However enterprises can take a systematic approach towards the IM technology[9].

- ***Secure IM session*** - Secure communication is a very big concern in any type of transactions occurring over IM. Organization should understand and document the level of security needed for the type of transactions that would be conducted using IM. This is needed in both, Public and Private IM. If organization is using public IM then the level of security needed may be higher than the Private IM. Private IM may not need 128 bit SSL encryption. But over Public IM network such higher level will ensure that message can be read only by the recipient.
  Just because organization uses private IM does not mean it does not need to secure internal IM communication. It just means that a lesser level of encryption may be adequate. 128 bit SSL encryption could be an over kill depending on the sensitivity of the communication. No encryption or low level of encryption could be used for the regular staff. Separate level of encryption could be used for executive or sensitive level of communication.

- ***Logging, Monitoring and Administration*** – This allows companies to create and maintain a regulatory-compliant record of all communications. Also the IT administrative controls help prevent viruses from entering corporate network by forcing incoming files to be scanned or by not allowing any files to be transferred. This also, allows administrators to enable/disable other system features. "Free IM services will be found in 70 percent of enterprises by 2003, and it will be implemented by end-users without IT organization sanction or support", according to Gartner, Inc[6].
  1. *Logging* – Most of the small businesses are using the existing public IM network services. In situations like these it is very easy to abuse the facility. Employees could be using company IM ID to conduct personal IM chat sessions. Log of IM session could be a step to prevent the abuse of

[9] Bird, Drew. "Choosing an Instant Messaging System". Instant Messaging Planet. July 16, 2003.
[6] Gartner Press Room. Press release "Gartner Says Free Instant Messaging will be Found in 70 Percent of Enterprises within Two Years". October 2001.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the IM, such facility is not currently available in Public IM. In some industries logging is part of the regulatory requirement. If a Corporation has specific logging requirements it is important that the IM system being implemented fulfills those requirements.

2. *Monitoring the use of IM* – Monitoring use of IM is very important. Lot of companies monitor private usage of telephone, Internet surfing, e-mail by their employees. IM usage among employees will also be monitored very closely by the enterprises. Such monitoring can be a concern in certain industries such as health care industry. Monitoring the usage could go against the individuals right to privacy.
3. *Administration and Record keeping* - Administration of IM usage could be a huge problem in an enterprise. Sometimes the IM sessions could become long and lengthy. It is important to archive the decision making process that occurred. For example, in financial industry the law requires that a proper record of every transaction be maintained. The cost of storage could be very high. Fortunately this is one feature that is offered in Public IM. During such business oriented records some of the personal information about a client or a vendor could be captured. Administration of IM could be done similar to e-mail administration. This could be a cost saving in terms of labor and time.
   However this needs to be evaluated carefully since it involves individual privacy rights. If IM is popular because of its interactive nature, the same interaction is undesirable due to its need to maintain the record trail. Just imagine a message that pops up before the IM session ' All IM session are recorded and monitored in order to provide you better service'. Would a customer dare to IM with you?

- ***Access Control***- Proper Access controls is the key factor to secure access to any network. Organization of any size should establish proper access controls in usage of IM by employees. The procedures should be identified and documented. Such policies and procedures should consider the following:
  1. *Level of access* – It is important to identify which and what level of employees can have IM access. The "read only" or "read and respond" to IM message could be limited to only employees in certain departments, such as customer service, sales etc.
  2. *Access authorization* – Access granted to select employees should be authorized by appropriate level of management. The flow of authorization should be documented and maintained on a regular basis.
  3. *Type of access* – Should the employees be allowed to use the IM services for personal use? If so that could mean employees trying to interact with other private or public IM networks. Security impact of such an access should be evaluated.
  4. *Means of access* – Should IM be installed on all desktops, laptops or wireless devices in the organization? Does organization need to restrict it to particular lab or to certain high level executive offices?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

5. *Record keeping* – Policy regarding the identification of the IM sessions on records or non-records should be in place. Such records should be properly labeled with the appropriate information. Also a guideline should be created for the length of time such records should be maintained.

- ***IM Interoperability*** – As e-mail in the beginning had interoperability issue, IM is currently facing the same problem. User of one IM vendor can not hold IM session with user of another vendor. In short, user on Yahoo Messenger cannot start an IM session with MSN Messenger user. This is a significant limitation in the commercial and public sector. For leading vendors like AOL this is not a great concern. They already have significant user base. More users will be willing to sing up due to stability of such long lasting networks. One of the reasons that have been given by AOL is that interoperability with other networks will expose its network to the greater security risk such as hacking[1].

  Due to various security concerns corporations are more likely to establish Private IM networks. This gives them ability to communicate on as needed basis with other private and public IM networks. Lack of single platform limits the options an enterprise can explore. Thus creates a very big concern in the business community. Lack of integration with other enterprise application makes it a very costly affair for the enterprise to implement IM based solutions.

  Currently the Internet Engineering Task Force (IETF) is involved in setting IM standards. The most popular industry wide IM standards are SIP and SIMPLE.

  1. <u>Session Initiated Protocol or Session Initiation Protocol (SIP):</u> SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, chat, interactive games, and virtual reality. The protocol initiates call setup, routing, authentication and other feature messages to endpoints within an IP domain[15].

  2. <u>SIMPLE stands for Session Initiation Protocol (SIP) for Instant Messaging and Presence Leveraging Extensions</u>: This is an application of the SIP protocol for server-to-server and client-to-server interoperability in instant messaging. SIMPLE is a step in bringing standardization to instant messaging[16].

---

[1] Bird, Drew. "Instant Messaging: Corporate Productivity Tool or Cool Toy? ". Intranet Journal, May 1, 2003.
[15] IETF.org. Session Initiation Protocol (sip). July 24, 2003.
[16] NetworkWorldFusion. SIMPLE (Session Initiation Protocol for IM and Presence Leveraging Extensions).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SIP and SIMPLE are the standards used by major IM industry leaders. SIMPLE standard seems to have potential of resolving the interoperability issue.

IM and other related products selected by organization need to integrate with its existing network and application interface. Functional interoperability will ensure steady and expected level of IM communication.

- ***Integration with other In-house application*** - The need of Integration of IM with other in-house application also should be considered. In order to make use of IM technology, IM may have to be incorporated with marketing, sales or customer support applications. Make sure that IM system being implemented can interface with the existing directory service. This can be used to ensure user authentication. Organizations focus should be on the present as well as future business & IT needs. Considerations to the future vision will help organization make an educated and selective decision about the integration of IM with existing in-house applications.

- ***Cost benefit Analysis*** - Most of the time cost is the deciding factor in implementation of new technology. Organization could decide to use IM in order to provide the best customer service. But if organization lacks money to implement such solution it simply cannot execute it. Cost benefit analysis will help in the selection of the appropriate IM products.

- ***Risk Analysis***- Risk is associated with implementation of any new technology. Especially something as immature as IM. Risk analysis of internal, external or commercial IM usage will provide a proper insight in to the risk associated with IM technology. Various scenarios and associated risk should be considered by the organization.

- ***Flexibility, diversity and dynamic product*** – Even if the IM technology is new it is important to buy the product that will grow with the organization. If bought from a reputed company such product will have initial muscle to stay in the market for the long haul. Such product can develop and integrate the new features faster. Such faster service means cutting edge technology advantage to the organization.

To plan and adopt IM technology in an enterprise in a secure manner several products have become available. Public IM vendors such as AOL, Yahoo and MSN offer Enterprise grade IM products. Also variety of products that interface with the existing Public IM networks are also available in the market. These products are good but do not yet offer all the solutions to organizations security problems. Organization still has to consider the features offered by these products and choose what suits their needs. InstantMessagingPlanet.com lists

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

some of the IM product available[10]. The following products seem to provide much needed solutions to various security issues discussed earlier in this paper.

Top Secret Messenger

Top Secret Messenger (TSM) is product developed by Encryption Software, Inc. It provides a powerful public-key encryption platform, one of the key features discussed earlier. TSM users do not have to perform any additional actions to encrypt and decrypt their messages, beyond the one-time initial and simple public-key exchange procedure. TSM uses 307-bit ECC private and session keys in its encryption.

TSM provides integrated add-on for popular instant messengers such as ICQ Instant Messenger (AOL), MSN Instant Messenger (Microsoft), Outlook Express and Outlook (Microsoft), and Miranda MSN and ICQ clone. TSM provides a choice to an organization, which utilizes Microsoft outlook for its e-mail system and is looking for enterprise grade secure Public IM product. This is a good example of integrating the new IM technology with existing system applications[11].

Vayusphere Managed IM Gateway

Vayusphere MiG provides controlled employee access to Public IM. It uses relational database to store public IM conversation. This feature allows enterprises to archive and search thereby satisfying the document retention and compliance requirements. Vayusphere MIG supports all major public IM networks including AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger. Vayursphere MIG allows creation of usage and traffic reports to dynamically track IM usage[12].

A.I.M. Frame

A.I.M. Frame runs on top of AOL's AIM. A.I.M. Frame records and logs all conversations with date/time stamp. IM logs can be integrated into enterprise databases via ODBC connection. A.I.M Frame also supports encrypted instant messaging to other A.I.M. Frame users. It is also equipped with some convenient features such as Auto spell check, send all, which let you send the same message to multiple users like an e-mail[13].

[10] Instant Messaging Planet: IM Products: Security.
[11] Encryption Software: Top Secret Messenger
[12] Vayusphere: Instant response for the real time enterprise. Product Vayusphere managed IM gateway
[13] A.I.M Frame Automatic Instant Messaging Frame for AIM

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary

Instant messaging is very popular and used very heavily for personal use by consumers. It seems like next logical step would be to use Instant Messaging commercially. There is a great potential for Instant Messaging products and services in the corporate world. Companies should evaluate the security needs in order to use Instant messaging for commercial purposes. A cost benefit analysis of security risk and the benefit achieved to increase productivity or profit will help companies decide the direction. Looking at the variety of products and services that are out in the market it is very clear that Instant Messaging is here to stay and the demand for IM will continue to grow over the next few years, as the technology becomes robust.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Bird, Drew. "Instant Messaging: Corporate Productivity Tool or Cool Toy? ". Intranet Journal, May 1, 2003.
   URL: http://www.intranetjournal.com/articles/200305/ij_05_01_03a.html (Aug 19, 2003).

2. Data points. AOL: the worlds leading interactive service. Who We Are.
   URL: http://corp.aol.com/whoweare/who_datapoints.html (Aug 19, 2003).

3. Microsoft, Press Pass. MSN 8 Butterfly Squad Nationwide Tour Takes Flight. Feb 13, 2003.
   URL: http://www.microsoft.com/presspass/press/2003/feb03/02-13butterflytourpr.asp (Aug 24, 2003).

4. "Relating in real time". Yahoo! 2002 Annual report.
   URL: http://yhoo.client.shareholder.com/ar2002/pro_ns_3.html (Aug 19, 2003).

5. Hallett, Tony. "IM creates 'rampant security risk'". ZDNet UK. February 5, 2003.
   URL: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20271831,00.htm (Aug 19, 2003).

6. Gartner Press Room. Press release "Gartner Says Free Instant Messaging will be Found in 70 Percent of Enterprises within Two Years". October 2001.
   URL: http://www.dataquest.com/press_gartner/quickstats/IM.html (Aug 19, 2003).

7. Vijayan, Jaikumar. "Users, Experts: IM poses Security Risk". COMPUTERWORLD. December 3, 2001.
   URL: http://www.computerworld.com/softwaretopics/software/story/0,10801,66264,00.html (Aug 19, 2003).

8. Desmond, John. "Report: Secure IM Alternatives Growing". eSecurity Planet: Trends. June 12, 2003.
   URL: http://www.esecurityplanet.com/trends/article.php/2221091 (Aug 19, 2003)

9. Bird, Drew. "Choosing an Instant Messaging System". Instant Messaging Planet. July 16, 2003.
   URL: http://www.instantmessagingplanet.com/enterprise/article.php/2236051 (Aug 19, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. Instant Messaging Planet: IM Products: Security.
URL: http://products.instantmessagingplanet.com/imp/security/recent1.html (Aug 19, 2003).

11. Encryption Software: Top Secret Messenger
URL: http://www.encrsoft.com/products/tsm.html (Aug 19, 2003)

12. Vayusphere: Instant response for the real time enterprise. Product Vayusphere managed IM gateway
URL: http://www.vayusphere.com/products-MiG.htm (Aug 19, 2003).

13. A.I.M Frame Automatic Instant Messaging Frame for AIM
URL: http://www.aimframe.com/ (Aug 19, 2003).

14. Jeff Tyson. "How Instant Messaging Works". Howstuffworks.
URL: http://computer.howstuffworks.com/instant-messaging.htm (Aug 24, 2003).

15. IETF.org. Session Initiation Protocol (sip). July 24, 2003.
URL: http://www.ietf.org/html.charters/sip-charter.html (Aug 24, 2003).

16. NetworkWorldFusion. SIMPLE (Session Initiation Protocol for IM and Presence Leveraging Extensions).
URL: http://www.nwfusion.com/links/Encyclopedia/S/799.html (Aug 24, 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: November 30th, 2015

Upcoming SANS Training

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

Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Cyber Defence Delhi 2016	**Delhi, IN**	**Jan 11, 2016 - Jan 22, 2016**	**Live Event**
SANS Brussels Winter 2016	**Brussels, BE**	**Jan 18, 2016 - Jan 23, 2016**	**Live Event**
SANS Security East 2016	**New Orleans, LAUS**	**Jan 25, 2016 - Jan 30, 2016**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Alexandria, VAUS**	**Feb 03, 2016 - Feb 10, 2016**	**Live Event**
SANS Scottsdale 2016	**Scottsdale, AZUS**	**Feb 08, 2016 - Feb 13, 2016**	**Live Event**
SANS McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Secure Japan 2016	**Tokyo, JP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
RSA Conference 2016	**San Francisco, CAUS**	**Feb 28, 2016 - Feb 29, 2016**	**Live Event**
SANS London Spring 2016	**London, GB**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS Philadelphia 2016	**Philadelphia, PAUS**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
HIMSS	**OnlineMAUS**	**Dec 01, 2015 - Dec 02, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**