



## Protecting Your Business From Instant Messaging

By Mark Bella

Instant messaging provides real-time communication between people via text over a network and also provides the ability to transfer files. Instant messaging has been looked at as an alternative to email and has been gaining popularity in both professional and personal environments. Instant messaging networks consist of clients and servers. Each client is given a unique identifier such as a name or number. The client establishes a session with the server by authenticating to the server. When the client attempts to communicate to another client on the network, it sends a packet containing the message to the server. The server then examines the packet and forwards it to the correct client.<sup>1</sup>

Instant messaging in a corporate environment can be viewed as a viable communication tool. Instant messaging promotes collaboration and real-time communication between employees, business partners and customers. In project environments, instant messaging can be used to answer questions in an instant rather than a series of phone calls, emails and meetings.<sup>2</sup> The Radicati Group estimates that 26 percent of American companies use instant messaging as an official corporate service, while an additional 44 percent acknowledge their employees use instant messaging as a form of communication.<sup>3</sup>

Instant messaging also introduces additional network security risks and subjects organizations to potential liability risks. In addition it can result in reduced productivity and significant drain on IT resources. Instant messaging is difficult to detect at the network level because it's often embedded in HTTP traffic.<sup>4</sup> It also goes undetected in organizations because individuals can sometimes load the client on their local computer. Similar to email, threats such as viruses, worms and Trojans can also be transferred through instant messaging. An infected computer can infect other computers, damage files, consume resources and potentially open up the entire computer system to other attacks.

In 2005, 90 percent of instant messaging security attacks were worms, 9 percent were viruses and Trojans and 1 percent were instant messaging client vulnerabilities.<sup>5</sup> The most common type of instant messaging vulnerabilities is a denial-of-service (DOS) attack. The DOS attack floods the client with messages with the intent of overloading resources on that computer or their network. The end result is most likely the instant messaging client crashes or the

---

<sup>1</sup> Security Focus - <http://www.securityfocus.com>

<sup>2</sup> WebSense - <http://www.websense.com>

<sup>3</sup> PC Magazine - <http://www.pcmagazine.com>

<sup>4</sup> Security Focus - <http://www.securityfocus.com>

<sup>5</sup> Clickz - <http://www.clickz.com>



computer freezes. Worms are self-replication computer programs designed to consume resources and propagate to other nodes. More damaging than denial-of-service attacks and worms, Trojans are designed to disguise itself and another program and install backdoor programs which allow unauthorized remote access. A hacker can gather confidential information such as a user's name, password, contact list and logs. With this information collected it's then possible to impersonate the user and gathering even more personal information. There have been several cases in which stolen logs contained sensitive or private information from past Instant Messaging conversations and caused damage reputations and even legal problems.

In addition to malicious attacks, the use of instant messaging also creates a risk of non-compliance to laws. Businesses have a legal responsibility to ensure a harassment-free environment for employees. The use of company owned computers, networks and software to harass an individual or spread inappropriate jokes creates liability for both the offender and employer. There are over 10,000 laws and regulations related to electronic messaging in the United States alone. Some of the well-known laws include the Sarbanes-Oxley Act, HIPAA (Health Insurance Portability and Accountability Act) and the Securities and Exchange Commission's 17a-3. The most common regulation related to Instant Messaging in businesses involves the need to produce archived communications to satisfy government or judicial requests under law. Failure to meet these requirements may subject businesses to fines, penalties and damages.<sup>6</sup>

There are several ways you can protect your business from the risks of instant messaging. The most effective way is to block instant messaging. Blocking instant messaging traffic on a firewall can prove to be difficult. Many clients use standard ports such as HTTP (Port 80), while other auto-configure to use random ports.<sup>7</sup> Clients can get around company firewall by using proxy servers from the internet. There countless proxy servers available and even come from major corporations such as AOL. Firewalls such as the Fortigate series from Fortinet ([www.fortinet.com](http://www.fortinet.com)) are capable of protocol analysis and can block or permit traffic based on the type of protocol used.

Although blocking would reduce most risks, some companies would prefer to use instant messaging within their organization. One method to help reduce risk is to encrypt the information being sent. Many popular instant messengers have enterprise versions which include encryption as an option. This would help prevent hackers from reading messages through packet sniffers or hijacking a connection. Encryption alone will not protect you against all threats. Viruses, worms and Trojans can spread through files transfer. It's highly recommended Antivirus agents are installed on all computers, whether it will be used for instant messaging or not. An infected computer can spread to other computers on the network.

---

<sup>6</sup> Wikipedia – <http://www.wikipedia.org>

<sup>7</sup>Symantec - <http://www.symantec.com>



Whether you decided to allow or block instant messaging, company policies should be established and communicated to all employees. This can help reduce many of the issues associated with instant messaging. If it's not officially stated, some users will go to extreme lengths to get instant messaging working. Others may disclose information the company might want not want the public to know. Ultimately it's up to the business to decide whether instant messaging in their business is worth the security risks compared to the advantages.