MESSAGING

Managing Your Instant Messaging Frontier

David Strom

As security and policy become more crucial issues, enterprises must be more sophisticated in managing IM and peer-to-peer traffic.

Instant messaging has become the next communications battleground for enterprise IT managers. IM use has exploded, well beyond pimply teens talking through the night—corporate IT staffs are actually building applications that take advantage of IM's real-time presence detection features.

As companies become comfortable with telecommuting and home-based workers, they are finding that it is IM, not email, that ties their staffs together and binds distributed project teams. And also, IM is more appropriate than an overwhelmed email inbox as a way to replace phone tag.

Look at IBM's internal deployment as an extreme example. Since installing its Lotus division's SameTime, "We send 2.5 million IMs within IBM each day," said David Marshak, senior product manager for collaboration at IBM and a former industry analyst. "And we have virtually zero voice mails here. What makes the difference is that with IM, you have the ability of getting an answer back immediately, rather than waiting, and getting a quick answer to your question."

But IM isn't just a voice-mail replacement. For corporations with Microsoft Exchange and IBM's Notes/Domino email systems, the IM/telephony integration is also compelling.

"Our telephony switch is only five years old, so replacing it with a full IP switch is not fiscally prudent," said Sam Blumenstyk, with the IT department at New York law firm Schulte Roth & Zabel. "What we like about IM/telephony integration is how it provides PC-based call management, so we can leverage our investment in our existing PBX."

David Strom is a freelance writer and author of two computer books and can be reached at david@strom.com. He uses multiple IM networks, including AIM, Skype, and others.

Increasing IM Usage

Ironically, it is this immediate gratification and fast response—which teenagers have known about for more than a decade—that has made IM attractive to corporations. And its corporate popularity is on the rise. Several surveys show IM is used in the vast majority of corporations today; more than 80 percent, according to one survey by Osterman Research.

There are several reasons for the growth in corporate IM use. First off, workers have become more mobile and a lot harder to track down. As secretarial support disappears and voice mail becomes more the norm, you want to know when someone is actually at his or her desk—or wherever—these days.

Second, email is no longer the productivity tool it once was, as pipes are clogged with spam and phishing attacks. Third, staffs are more far-flung, and the global village becomes a lot smaller when you can IM someone halfway across the planet and get an immediate response.

Fourth, the next generation of IM is not just about text chats, but offers solid integration with voice and video, too. Finally, IM's real-time features and the ability to track someone down no matter where they are located, have proven attractive to customers, partners and suppliers who need a guaranteed method of communication.

As an example, take an ecommerce site such as that offered by Accredited Home Lenders, which offers IM features to its potential customers looking for mortgages. For Accredited Home Lenders, mortgage brokers can work with loan specialists in real-time to resolve issues with loan applications and provide up-to-the-minute application status information.

"We have seen significant increases with retailers that are using IM and getting higher percentages of purchases on their websites," said Joe Heinzen, the president of e-Convergence Solutions, a distributor that specializes in IM solutions.

But IM has its down side too: Being on someone's buddy list is a small but powerful indication of trusted identity, and that means that some malware masquerading from such a trusted buddy can easily gain access into a corporate network and infect thousands of machines in seconds. Most IM systems are adept at crossing firewalls and skirting ordinary intrusion prevention systems with nary a care, which makes it harder for corporate IT staffs to control their usage and block access completely. And its real-time blessing is also its curse, as prophylactic measures need to keep up to date and be wary of the latest exploits.

And you can be sure these exploits are on the rise as corporate IM usage grows. "IM has finally got the attention of hackers, now that it has a critical mass in the workplace," said independent IM analyst Michael Osterman.

According to Akonix Systems' IM Security Center, 328 threats using IM as an infection vector were recorded during 2005; that's up from a mere 21 during all of 2004. Furthermore, when you include instant relay chat (IRC) and peer networking mechanisms, the number of threats observed last year is more than 2,500. And the rate continues to climb.

"IM is the application that people are using, but the peer-to-peer file sharing applications are where most of the threats are coming from," said Don Montgomery, VP of marketing at Akonix. "P2P networks are the real breeding grounds for trojans and worms."

Protecting IM Applications

The solution for IM protection is typically an appliance or dedicated Linux server running some software to detect, manage and block IM traffic across corporate networks. The largest vendors in this area include Symantec—which just recently purchased IMLogic—competing with Akonix and FaceTime.

Given the fact that IM threats are closely related to P2P, FaceTime has branched out and taken a broader perspective. "Our focus is on managing and securing grey networks," said CEO Kailash Ambwani. "Grey" networks—so called because they are inherently neither malicious (i.e., black) nor benign (white)—include peer to peer networks that share files, or applications such as Skype that use peering technology.

"IM is an important piece of what we do, but it isn't the only thing," Ambwani said. "We want to protect against everything that an end user can bring into the enterprise, and block malware and spyware whatever the vector.

"Because they are evasive on the network, and open up channels inside your organization that are difficult to control, they represent potential vectors of malware," Ambwani concluded.

The focus must expand from IM to P2P

How To Select Your IM Security Product

Before you purchase any IM protection products, ask your prospective vendor the following questions:

1. What IM products are covered?
Not all IM networks are treated equally by the IM security vendors. "We cover AOL, MSN, Yahoo, and Google Talk and other IM clients that work with those networks, like Trillian," said Art Gilliland, VP of product marketing with IMLogic. "But with Skype, we can't manage it—we can only block it. We hope to fully support them within the next nine months."

If your end user population is starting to use Skype or other peering networks, then consider those vendors that have protection here—most notably, Akonix, FaceTime and IMLogic.

2. What threats aren't covered by your existing intrusion protection systems (IPSs)?
Intrusion protection systems aren't perfect. "IPSs and IDSs [intrusion detection systems] don't always work for IM threats," said Gilliland. "A lot of time virus traffic looks like safe traffic over IM. For this reason, you need security at multiple layers and at multiple points across your network." The elements of this layered approach are firewall, client and server. This protects both the UDP and IP network layers.

3. What happens when people use Web IM clients?
Most of the IM systems have Web-based clients or clients that run on mobile phones and PDAs. "IM clients can be resourceful," said Michael Osterman, an independent IM analyst. "If you block port 80 [which Web traffic uses], you can unintentionally block legitimate Web traffic, so you have to do more sophisticated things." How the security system manages and blocks this kind of traffic is important, as infections can just as easily spread from these sources. So the "sophisticated things" may include looking at the destination servers that the Web clients are connecting to, the protocols and proxies that they are using, and blocking these entry points.

4. How is reporting done, and what reports are available?
Each product has a different range of reporting capabilities and features. Some reports are Web-based, others use SQL databases to track attacks. And if you are deploying IM security for compliance or other legal reasons, you will want to have your system produce appropriate reports. Systems can report on time of infection, IP address of source, application of source; some can do more than block an application, say, restrict it to a given group of users or IP ranges, for example.

5. How often do you update your exploit signature base?
Each vendor handles updates differently: some update several times a day, others only once a week or a few times per month. The more frequent the updates, the more on top of threats your system will be. "We update our signature database quite frequently," said Gilliland of IMLogic. "The default is every two hours, but we can do it every 60 seconds."□

Greater interoperability among IM services will create new security headaches

Fortunately, picking the right IM security product isn't difficult, and the sidebar, "How To Select Your IM Security Product," (p. 63) offers several suggestions on how to choose.

Future IM Trends

IM will go through further changes in 2006, as a result of four major trends coming together:

- The increase in cross-systems connectivity.
- The mashing together of IM with voice over IP solutions such as Skype.
- The rise of open source IM software.
- The deployment of very large-scale internal IM networks by major corporations.

Let's look at each trend and see what it means for corporate IT managers who are trying to protect their networks.

The world of today's IM is not unlike the world of email in the early 1990s. Back then, there were several proprietary systems with their own clients, protocols, and authentication and identity systems. Remember MCIMail, Compuserve, The Source, and even cc:Mail and Higgins? All of these are gone today, subsumed by the Internet and standard protocols that enabled emails to be sent across the world without having to go through specialized gateways and translations.

The same is becoming true for IM. There are several major proprietary systems with their own clients, including AOL Instant Messenger (AIM), Microsoft, Yahoo and Skype. Being a member on one of these systems doesn't buy you any connectivity with buddies on a different system. These vendors have done all they could to keep their walls up and competitors out. And while there are multiple-client products such as Trillian and GAIM, you still need to provide your login credentials to each network.

Nevertheless, the walls are coming down. IBM announced earlier this year that its SameTime product would widen its support beyond AIM, and include other networks too. Google and AOL are working on common solutions. And hope springs eternal that even Microsoft will open its IM doors. All of this will make IM security even more critical as buddy lists widen beyond single networks.

Trend number 2 has to do with Skype, and what it has accomplished. Skype combines peering networks with voice and text chat and is very good at getting around roadblocks and firewalls (provided that third-party blocking solutions aren't installed). It now has several million concurrent users at any given point during the day.

"Skype is regarded as a threat by many companies right now, and opinions range from it being a great productivity tool all the way to a very complex piece of spyware," said Osterman. "But it isn't just Skype. Any consumer-grade solution that sends voice over IP is potentially a serious threat that can bypass the corporate security."

Osterman said corporations should have a Skype strategy, especially since Skype was acquired last year by eBay and usage continues to climb. As an example, some IM security products are only able to offer the choice of blocking vs. allowing Skype conversations; in contrast, other packages are more adept at managing other IM solutions.

But Skype isn't the only fast-growing IM/voice combination. The open source community isn't standing still, and they are hard at work to establish a more pluralistic IM society.

These efforts revolve around software called Jabber and the protocol called the Extensible Messaging and Presence Protocol (XMPP). XMPP is the IETF's formalization of the core protocols created by the Jabber open source community in 1999, and is contained in four RFCs, beginning with number 3920.

Jeremie Miller developed the original Jabber server back in 1998. Now the project has reached critical mass and has dozens of different client implementations. Last year, support reached a new milestone, with Google Talk and more recently the Gizmo Project (a freeware softphone) using these protocols.

Finally, some companies may want to deal with the potential risks by barring all public IM traffic. These enterprises can still gain the communications and productivity benefits of IM by using an internal IM solution that has little or no connectivity to the popular and public IM systems. Most companies that deploy a private IM solution also use IM security products to block public IM clients as a matter of policy.

Conclusion

Just like Trix cereal, IM isn't just for kids anymore and has come of age for corporate users. "Just like we cannot do without email these days, IM has become another critical communications medium for our firm," said Blumenstyk□

Companies Mentioned In This Article

- Accredited Home Lenders (www.accreditedhomelenders.com)
- Akonix (www.akonix.com)
- AOL (www.aol.com)
- eBay (www.ebay.com)
- e-Convergence Solutions (www.econvergencesolutions.com)
- FaceTime (www.facetime.com)
- Gizmo Project (www.gizmoproject.com)
- Google (www.google.com)
- IMB (www.ibm.com)
- Jabber (www.jabber.org)
- Microsoft (www.microsoft.com)
- Skype (www.skype.com)
- Symantec (www.symantec.com)
- Yahoo (www.yahoo.com)