Endeavors TECHNOLOGY

Locking and Blocking

Secure IM Countermeasure Architecture Issues

A White Paper |

Gregory Alan Bolcer
Chief Technology Officer, Endeavors Technology, Inc.

2002 © Endeavors Technology Technologies, Inc.

Instant Messaging (IM) is proving to be no longer a consumer phenomenon. With over 40 million enterprise users, it is becoming de rigueur as a real-time business collaboration tool.

To date, enterprises have had to make the hard choice between inside-the-firewall, self-managed solutions with little or no external interaction or an outside-the-firewall approach with little or no security, trust, or control. Enterprises refusing to land on either side of the issue have resorted to draconian measures to lock down IM use at a great expense to their users. This has met with very little success due to the ease of which users can circumvent these policies.

This white paper covers some of the social and technical issues surrounding this hot button topic as well as some of the choices enterprises are making. These choices become increasingly important as history provides us with a not-so-subtle guide to adopting technologies that work across trust boundaries, provide cross-organization benefits, and yet allow IT control. Like enterprise email adoption from 1985-1995 or Web server adoption from 1991-1997, enterprise instant messaging is at a point in its adoption cycle where organizations are starting to see value in extending it securely beyond their current borders.

ABOUT THE AUTHOR

GREGORY ALAN BOLCER is a co-Founder of Endeavors Technology, Inc. and is currently its Chief Technology Officer.

At Endeavors Technology, Dr. Bolcer founded the Magi™ project, a lightweight, open protocol, thin server infrastructure for forming ad hoc, peer-to-peer networks and accessing embedded systems through standard Web protocols.

Prior to co-founding Endeavors Technology, Dr. Bolcer's research team at UCI received $4 million in grants from the Defense Advanced Research Project Agency (DARPA). His project at one point was the largest Java-built, non-Sun Microsystems project in the country. He was one of the key working group participants and co-Author for the widely supported Simple Workflow Access Protocol (SWAP/WF-XML) extensions to HTTP/1.1 and WebDAV (the Web Distributed Authoring and Versioning Protocol).

Dr. Bolcer has a PhD and BS degree in Information and Computer Science from the University of California, Irvine, and an MS degree from the University of Southern California.

2002 © Endeavors Technology Technologies, Inc.

Introduction

- **Locking Down Desktop Software**
- **Perimeter Firewall**
- **Enterprise Policy**
- **Spot Audits**
- **Trusted Gateway**
- **Authenticated Network Access**

The ***good news*** is that most enterprises already have all the tools they need to block IM usage without buying new software. The ***bad news*** is that eliminating 100% of IM usage in an enterprise is a near impossibility. Because of this, Endeavors highly encourages enterprises to pursue a strategy of locking & blocking. This is often called a "carrots and sticks" approach. The "*carrot-on-a-string*" creates incentives such as the ability to utilize IM services for adhering to an enterprise's policy. The "*whack-them-with-a-stick*" allows IT to have some level of enforcement. Locking is done through secure authentication, encryption, provisioning, and auditing. Blocking is done through a few simple IM countermeasures as configured by an enterprise's IT staff.

Limiting IM usage to inside-the-firewall only usage is about as productive as restricting email recipients to only others at the same company or allowing only Web traffic to pre-approved sites. Outlined here are some of the steps an enterprise IT manager can take to get IM back under IT control. Depending on the enterprise culture, some of these steps have undesirable consequences on employee morale or productivity or IT time and management. Endeavors is proposing a solution architecture that avoids IM client switching & redeployment costs, allows IT to tie public IM identities back into enterprise ones, and requires a minimum amount of infrastructural change.

Locking Down Desktop Software

The simplest way to prevent employees from running a program is to control the software that they run via a standard operating system image. Even in the best circumstances, only 70% of an enterprise will run the default OS image without any changes or modifications. It's inevitable that different users need access to different software. Controlling software installation through IT involves delivering every desktop with administrative privileges turned off. This means that even simple upgrades, driver updates, bug fixes, patches need to be routed, automatically or not, through IT, which can create a backlog of end user requests. Many recent OS versions already come default with IM clients bundled into the installation causing IT removal of IM clients to be an added burden. Many enterprises will grant users software installation privileges at the desktop to ease IT burdens. This is often combined with a policy of limiting help-desk support for non-standard tools or configurations.

2002 © Endeavors Technology Technologies, Inc.

Perimeter Firewall

One of ways enterprises are trying to block IM usage is through blocking access to specific public IM machines or restricting traffic through known ports that these services use. Modern IM clients all support messaging and traffic on currently unrestricted Web and secure Web ports. The problem with this is that this leaves IT with ***two choices***: **1)** *filter all incoming and outgoing network traffic* or **2)** *use a network intrusion system* that watches for IM patterns as they go through the public network ports. Even with these tools, it's so easy for most enterprise users to get an outside network connection off to a Web site, that any "enterprising" IM user can simply connect to a Web proxy on his or her home system through their DSL connection to get around a perimeter firewall. Because of this, blocking ports at the perimeter without controlling the desktop or vice versa isn't very effective at all for enforcing IM use policies. Some best practices for controlling some default installations are below.

AOL Instant Messenger	*IM* *Voice IM* *Chat* *File transfers* *Images*	Block port 5190 for version 4.x; new versions use any open ports and default to Web ones such as 80, 443; blocking inbound & outbound 4443 prevents image sending; blocking or resetting DNS for login.oscar.aol.com on all ports prevents sign-on
Microsoft Messenger	*IM* *File transfers* *Voice IM/chats* *Application sharing*	Block port 6891 for file transfers; block UDP ports 13324 and 13325 for voice; block TCP 1503 for app sharing; block TCP 1863 ports to hotmail.com messaging hosts (may prevent legitimate traffic)
Yahoo! Messenger	*IM* *Voice IM* *Chat*	Block inbound & outbound TCP 5010 for file transfers; block all access to yahoo.com messaging hosts (may prevent legitimate traffic)
AOL ICQ IM	*IM* *File transfers* *File sharing*	Block inbound & outbound TCP 5190, UDP 4000, TCP 4001 for previous versions; block TCP 3574 for file transfers; block TCP 7320 for file sharing; block all access to login.icq.com

Enterprise Policy

The single most effective tool IT has for controlling IM usage is establishing an acceptable IM usage policy. Compliance numbers typically range from 50%-90%, but degrade significantly as enterprises attempt to enforce an outright ban on all IM usage. Analysts estimate that less than 6% of time is spent on non-work related activities for all communication mediums including email, telephone, fax, and IM. Users generally will try to comply with enterprise policies, and in addition, users will self-modify their own behavior if they know that communication is being recorded or audited.

2002 © Endeavors Technology Technologies, Inc.

Spot Audits

Spot Audits allow IT to determine the compliance percentage of their policy. This in conjunction with an enterprise policy lets IT determine the effectiveness of certain dictates. This random enforcement tool allows IT to educate their users to the enterprise policy. Spot audits typically can be done through backup or asset management tools. Other spot audits can be done at the network level where a network "sniffer" such as the open source Ethereal tool can be used to determine the extent of non-approved IM usage.

Trusted Gateway

A trusted gateway is a central proxy that requires an authenticated username and password before proxying the network traffic. A trusted IM gateway can be setup in two different ways. The first is forcing all the IM clients to explicitly set the proxy value. This when combined with perimeter firewall blocking will prevent the majority of IM clients without this setting to work less efficiently or not at all. IM clients that use the proxy are allowed the full suite of functionality. The second way is to change the internal DNS settings inside the enterprise to remap all IM sign-on to pass through this trusted gateway. This is accomplished by setting DNS entries such as login.oscar.aol.com to map to an inside the firewall gateway machine. This gateway machine can then be the checkpoint for enforcing authentication using the enterprise's directory services such as LDAP, ActiveDirectory, or even and enterprise's email servers.

Authenticated Network Access

Many enterprises monitor and filter all outgoing traffic. Any enterprise user wanting to access the network, inside or outside, will need to undergo authentication. Typically this is done through a network or domain sign-on. Unlike a trusted gateway that is specific to a particular tool, this gives enterprises the ability to actively monitor network access by individual users. When a user signs onto the enterprise network, a combination of network spot auditing and authentication can be triggered to ensure proper policy compliance.

Magi: Authenticate, Encrypt, Block, Audit

Bringing IM back under IT control is a complicated issue. Many of the tools available to IT require expensive setup and deployment with limited effectiveness or benefits. Magi balances the cost of complete IM control with the benefits of addressing the most critical problems facing enterprises with regards to IM—namely ensuring intellectual property is properly handled such that confidential information isn't sent insecurely across public networks, ensuring that IT has at least the same amount of controls for IM as they do for email, and that public IM identities are referenceable to enterprise identities such that users have a way of knowing who they are instant messaging without having to give up the ability to quickly discover and contact others through the public services. Magi's leverages existing IM client's inherent support for HTTP, HTTPS, and SOCKS proxies. Magi transparently puts a trusted, authenticated proxy on the individual's machine that's also centrally controlled. This has the following benefits.

2002 © Endeavors Technology Technologies, Inc.

Authenticate.

A user or IT manager will install this trusted, desktop proxy which works transparently with existing IM tools. At installation time, the user will need to put in their identity and password for the sign-on server which can be an LDAP, ActiveDirectory, or email server. On successful authenticated network access, the Magi installation tool generates a unique set of RSA compliant, X.509 keys to underwrite the AIM or Microsoft Messenger username. Magi installation also automatically sets the proxy settings for the IM client. This mapping is then maintained by Magi, and users can now identify IM buddies by their enterprise identity. Individual clients can be revoked using certificate revocation.

Encrypt.

Because Magi puts a public and private key on the desktop, any IM or chat messages can be sent directly point to point via an SSL-encrypted pipe. Magi is built on top of the RSA SSL libraries which allow any encryption length. IT has the options of allowing or disallowing secure-to-insecure IM traffic. Individual presence information is sent to the public IM service under the public IM identity to allow for easy discovery, but no proprietary identities or information is ever sent over public networks. In addition, secure file browsing or sending is also permitted via Magi. Our strictest adherence to Web security and standards means that an enterprise's IM security is exactly the same as financial-grade Web security. Because both infrastructures work on the exact same well-tested technologies in use by tens of millions of extranets and e-commerce sites, the security exposure to the enterprise is capped by well-known security assurance issues.

Block.

Magi isn't per se an IM blocking tool by itself, but it can be used as part of an enterprise IM deployment. Magi can be configured to support secure IM traffic on specific ports through the firewall and default ones beyond. This allows the ability for enterprises to flexibly deploy the exact level of blocking that is required. The Magi client-resident proxy automatically starts when Windows does. This allows Magi to check for changed proxy settings in the IM client and sends a notification to the auditing server. The ability to have strong credentials tied to a public IM identity gives IT the ability to block unauthenticated IM traffic at any point in the network.

Audit.

Like email or Web sharing before it, IT needs the ability to make sure that IM is being used appropriately within the context of the enterprise. Recording all IM and chat sessions for auditing purposes is done by sending all messages directly to a Magi transcription server. This server uses JDBC to connect to any underlying database including Oracle, MySQL, Siebel, DB2, Sequel Server, etc. Magi provides default Java Server Pages for submitting queries on specific users or content, viewing session specific content, viewing any alerts for disabling the Magi software, setting up client-specific restrictions, or viewing file transfer logs. In addition, Magi has been tested against Crystal Reports, Access 2002, and Actuate with the proper SQL drivers to allow dynamic, customized report generation.

2002 © Endeavors Technology Technologies, Inc.

About Endeavors Technology

Endeavors Technology grew from research carried out at the University of California, Irvine, and was partly funded by the United States Defense Advanced Research Project Agency (DARPA). Endeavors' founders and technical advisory board has an unrivaled history in developing Internet infrastructures, both as co-authors of the Web's more commonly used protocols and software, including HTTP, Web Distributed Authoring and Versioning (WebDAV) and the Simple Workflow Access Control (SWAP/WF-XML), and as team members of the Apache Web Server project.

Endeavors Technology, Inc. is a wholly owned subsidiary of Tadpole Technology plc (LSE-TAD, www.tadpole.com), which has offices in Irvine (California), and Cambridge, Edinburgh, and Bristol (UK). Endeavors' Magi technology transforms today's Web into a highly secure inter- and intra-enterprise collaboration network for the delivery and interaction of files, Windows applications and instant messaging. For further information on Endeavors' Web software, call 949-833-2800, email to info@endeavors.com,

Endeavors Technology Inc.

North America:
19600 Fairchild, Suite 350
Irvine, CA 92612
Telephone: (949) 833 2800

Europe, Middle East and Africa:
Trinity House
Cowley Road
Cambridge, UK CB4 0WZ
Telephone: 44 1223 393 552

www.endeavors.com

This material contains proprietary information embodying substantial creative efforts and confidential information, ideas and expressions by the staff of Endeavors Technology Technologies, Inc. This is being distributed only as an informational aid to potential Endeavors Technology customers who want to make an informed decision relating to the purchase of the Magi Application Express product. This material may not be distributed or reproduced, in whole or in part, for any other purpose, without permission in writing from an Endeavors Technology corporate officer.