Security Analyses for Enterprise Instant Messaging (EIM) Systems

Joon S. Park and Tito Sierra

Consumer instant messaging (CIM) services (aka public IM) such as AOL Messenger, Yahoo! Messenger, and MSN Messenger have achieved critical mass appeal and usage as a convenient and informal method of communication supporting real-time messaging and presence awareness. Unfortunately, these services are highly vulnerable from a security standpoint. Some of these security problems include threats from viruses and worms, Trojan horses, identity theft, impersonation, eavesdropping, data loss, and denial-of-service attacks.

The increasing use of instant messaging in the workplace has increased concerns about security related to its use. Recently, AOL and Yahoo! announced that they will be pulling back from their EIM (enterprise instant messaging) businesses because of the concerns that enterprise IT managers have about IM management, including security vulnerabilities. Additional requirements of corporate instant messaging include protection of internally communicated information from unauthorized disclosure, protection from corporate espionage, government-mandated logging requirements, etc. To service these additional requirements, many companies have developed enterprise-grade instant messaging software solutions that promise more secure instant messaging environments. These solutions, collectively known as enterprise instant messaging (EIM) solutions, increase security by enabling greater local centralized control and by supporting additional security features such as encryption or digital certificates.

This article focuses on security issues related to instant messaging, first examining the threats and available countermeasures present in existing CIM services. These include viruses and worms, Trojan horses, identity theft, impersonation, eavesdropping, data loss, and denial-of-service attacks. This article then examines the variety of EIM solutions available. At present, four architectural models exist for EIM: (1) Gateway Policy Enforcement, (2) Internally Deployed EIM, (3) a Hybrid Solution, and (4) Managed Centralized EIM. Following this market analysis, the article considers these four classes of solutions in terms of their access control, authentication, messaging sessions supported, message routing, encryption, client software, interoperability with CIM, performance, and points of...
failure. Then, for each architecture, this article evaluates how that breed of EIM solution counters the aforementioned vulnerabilities, while also considering what new threats might emerge from the use of these new instant messaging platforms. Finally, the article concludes by considering the requirements for a high-security instant messaging system.

CONSUMER INSTANT MESSAGING (CIM)

CIM Overview

CIM applications are often referred to as peer-to-peer (P2P) applications because individual clients appear to communicate with each other directly in real-time. Two basic classes of P2P networks exist: (1) “pure” P2P and (2) “brokered” P2P.5,6 Pure P2P networks are self-organized networks that operate without centralized control mechanisms; examples include Gnutella and KaZaA for file sharing. Brokered P2P networks actually utilize a specialized form of client/server architecture that is optimized for client-to-client interaction. Brokered P2P networks typically use centralized servers for authentication, peer discovery, lookup, and messaging functions. Napster was an incredibly popular brokered P2P network used for file sharing.

CIM networks are brokered P2P networks. The infrastructure of a typical CIM service (see Figure 1) consists of two or more centralized servers that handle the authentication, presence tracking, and message routing functions that make up an instant messaging service. To date, implemented systems have been largely proprietary, although efforts are now being made to develop nonproprietary instant messaging networks.

CIM Security Threats

CIM networks and services are vulnerable to a variety of security threats. This section summarizes the threats that exist today:
viruses and worms, Trojan horses, identity theft, impersonation, eavesdropping, data loss, and denial-of-service attacks.

**Spreading Malware.** CIM client applications typically support the ability to transfer files, and not just text, between users. The file-sharing function has encouraged the development of instant messaging viruses, worms, or Trojan horses that use CIM networks as a channel for spreading malicious code.

A Symantec Corporation white paper states that more than 20 worms can be spread via instant messaging. This paper concluded that “instant messaging is an up and coming platform for malicious threats” based on the increasing number of worms targeting instant messaging each month. Particular exploits target specific CIM networks and software clients. As a result, some CIM networks are more vulnerable than others. According to Symantec, MSN Messenger is the instant messaging network that has the largest number of worms.

One widespread MSN Messenger worm that has received attention in the trade press is the so-called Choke worm. The Choke worm spreads by asking users to download a file called ShootPresidentBUSH.exe. If the user accepts the file, the worm spreads to people on the user’s buddy list. The use of the buddy list to spread the worm is analogous to the use of address books in e-mail-based worms; except that in the Choke case, human intervention is required for the malware to spread. Because of the need for manual intervention, Choke would be better classified as a virus rather than a worm, although the spreading behavior appears to be “worm-like.”

Trojan horses are another type of malware that can spread via the file sharing function, which is standard in most CIM applications. Trojan horses are malicious programs disguised as benign programs so that an unsuspecting victim will accept them on his or her own computer. Once accepted, the Trojan horse works silently to change settings on or steal information from the infected computer.

Classic Trojan horses open incoming and outgoing communication ports on the infected machine, thus allowing direct, surreptitious communication to occur between the attacker’s remote machine and the victim’s machine. This connection can be used to issue specific commands on the victim’s machine, such as changing file permissions, or to transmit stolen information or files back to the attacker’s machine. Trojan horses that target specific CIM client applications can use the CIM client itself to transmit stolen information. Trojan horses that utilize CIM clients as a communications channel are more difficult to detect because no suspicious new ports are opened.

**Identity Theft and Impersonation.** Trust in instant messaging is based on a communication history between users. CIM clients collapse the communication history between two users through the use of screen name identifiers. The lack of linking to true identifiers in the CIM client makes it difficult to detect identity theft when it occurs. If an identity thief is able to crack a user’s CIM username and password and log in under the stolen name, the victim’s CIM buddies may not be able to tell the difference.

For example, assume that Alice has regular secure instant messaging communications with Bob. Alice identifies Bob’s presence on the AOL CIM network based on Bob’s screen name “BobSmith123.” A third-party identity thief (Steve) cracks Bob’s username and password and logs into the CIM network as “Bob123.” Alice will assume that “Bob123” is Bob himself unless Steve reveals otherwise by engaging in messaging that is uncharacteristic of Bob. While logged in as Bob, Steve can leverage the trust Alice has in Bob to gain access to sensitive information that comprises either Alice’s or Bob’s security. In this example, if Bob is Alice’s boss, the information disclosure that occurs can easily include sensitive...
corporate information. Alternatively, Steve can take advantage of his assumed trusted position to initiate a Trojan horse attack on Alice via file sharing.

Because CIM services do not require formal identity registration, anyone can easily register an account with the existing CIM networks under an assumed name. The lack of formal identity registration can be abused by individuals to impersonate someone known to a potential victim for the purposes of stealing sensitive information or initiating sabotage. The impersonation threat in CIM services operates similarly to identity theft. In both cases, a third party assumes the identity of one user to gain the trust of another user. The difference is that an impersonator need not crack the password of a user to impersonate him or her. Instead, the impersonator registers with the CIM service provider under an assumed name, and initiates messaging requests to victims’ buddies under the new identity.

For example, assume that an impersonator (Steve) knows that a relationship exists between Alice and Bob. Assuming that Alice does not already have Bob on her buddy list, Steve can go to the CIM service provider Web site and register a new CIM account under Bob’s name. Because the CIM service does not require proof of Bob’s identification, Steve can impersonate Bob in the registration process and select the screen name “BobSmith321” (assuming it has not been previously registered). Steve then initiates an instant messaging request to Alice, pretending to be Bob. Alice may choose to add Bob to her buddy list and engage in a conversation solely based on the “BobSmith321” screen name. Steve can use this opportunity to compromise the security of Alice and Bob as described in the previous section.

**Eavesdropping.** CIM services typically transmit messages in cleartext over the public Internet. An eavesdropper can intercept messages at various points in the communication pipeline. For example, packet sniffer software can intercept the contents of many messages near the CIM centralized message routing server. Alternatively, a specific individual’s message content can be intercepted at the local network level for a targeted eavesdropping attack.

Suppose Alice has regular secure instant messaging communications with Bob using a CIM client at work. Assuming an eavesdropper (Steve) is able to install a network sniffer on Alice’s company network, he will be able to specifically monitor or log the communication session between Alice and Bob. Alternatively, Steve can eavesdrop on all CIM conversations taking place within the company until the sniffer is identified. This can be particularly damaging in a workplace setting if CIM is used by employees to communicate sensitive corporate information.

**Other Threats.** A core value of IM services is the presence awareness function. Presence awareness — knowing when someone is online and available to chat — is a requirement for the initiation of real-time communication. Unfortunately, presence information can be used to compile a profile about a user’s online behavior (i.e., when a user is online or offline). The profiler can then combine online presence information with other basic information, such as work schedules, to track the victim’s physical location.

Instant messaging denial-of-service (DoS) attacks can occur in several ways. A common DoS attack is to flood a particular user with a very large number of messages, potentially crashing the user’s client. Another type of attack will consume a large amount of the victim’s CPU power, thus causing the victim’s CIM application or entire computer to experience serious performance degradation. Using either method, the attacker can succeed in preventing the victim’s legitimate use of the CIM service.

**Possible Countermeasures to CIM Security Threats**

**Block Use Completely.** The simplest and most effective countermeasure to the threats...
discussed above is to block the use of CIM applications completely. Although this solution is straightforward to implement on an individual level (i.e., uninstall CIM clients), it can be challenging to enforce in the workplace. A clear corporate policy regarding instant messaging use is necessary, although insufficient. Many employees may be unaware of the threats of CIM usage, or may decide to ignore organizational security policy regarding CIM usage altogether.

A more direct approach to preventing CIM use in the workplace would be to block employees from connecting to these services in the first place. A firewall can be configured in several different ways to block internal users from connecting to external CIM servers. One strategy would be to configure firewalls to block all Internet services except for those services necessary to run the business — typically SMTP for e-mail and HTTP for Web access. This would block employees from sending or receiving TCP/IP traffic, which is the standard protocol used by CIM service providers. Unfortunately, however, the major CIM providers also include support for communications over HTTP if TCP/IP connections fail, enabling employees to connect to CIM services with the same protocol used for standard Web requests. A more effective strategy is to configure firewalls to block external communications with specific CIM service provider network addresses. This solution would require the company’s network administrator to know the DNS server names or IP addresses of each and every CIM authentication server to be blocked. However, if we assume that these addresses might change over time, this blocking strategy would require significant administrative overhead.

**Threat-Specific Countermeasures.** An alternative approach to blocking IM entirely is to try to mitigate the risks of the various vulnerabilities outlined in the previous section entitled “CIM Security Threats.” This threat-specific countermeasure approach is less secure than a total blocking of CIM traffic; however, if IM is a critical facet of the communications that facilitate the company’s operations, blocking CIM use completely may not be an acceptable solution to the security threats associated with CIM services. Moreover, while blocking CIM may be good for security, it is often bad for workplace morale. Consequently, to provide CIM in a sufficiently secure manner, strategies must be employed to counter each individual vulnerability. These countermeasures are limited, however, and in some cases no suitable remedy exists. In many cases, the countermeasures rely on the diligence of individual users.

Currently, for example, all instant messaging worms require user interaction for execution. In theory, greater user awareness of the threats posed by worms would reduce the severity of their damage. If users refused to open attachments sent by strangers, these worms would not spread. Unfortunately, past experience has shown that many users continue to actively spread these worms without knowing it. For these users, desktop anti-virus software provides a last measure of protection. Like viruses and worms, Trojan horses require user interaction for execution. Thus, to protect against Trojans, individual users need to exercise caution with those from whom they accept file-sharing requests.

However, no integrated security countermeasures exist for identity theft, impersonation, presence tracking, eavesdropping, and denial-of-service vulnerabilities. Identity theft victims must avoid disclosure of their password to minimize that threat. To mitigate the threat of impersonation and presence tracking, individual users need to exercise caution with regard to who gets added to their buddy lists. This lack of comprehensive and integrated security countermeasures to threats posed by CIM usage in the workplace is the main reason for the emergence of enterprise instant messaging (EIM) solutions.
EIM Overview

The proliferation of CIM usage among employees in the workplace has forced many companies to take notice of the security issues associated with these applications. Some companies have recognized the value of instant messaging as a collaboration tool, and have sought ways to exploit it more securely. Others are less sure of the benefits of instant messaging but still recognize the need to have more control over its usage in the workplace. As a result, many vendors have introduced the concept of enterprise instant messaging as a way to provide more secure instant messaging functions in the workplace. At the time of this writing, there are more than ten major EIM solutions in the marketplace (see Table 1), although AOL and Yahoo! recently announced that they will be pulling back from their EIM businesses because of the concerns that enterprise IT managers have about IM management, including security vulnerabilities.3,4

Different EIM solutions support similar security features but there are significant differences in how the various EIM solutions are implemented from an architectural point of view. This article proposes a classification of four major EIM architecture types. This classification of four architectures is derived from an analysis of product specification and technical documentation made available by vendors on the Internet. Table 1 groups ten major EIM solutions according to their implementation architecture.

An analysis of architectures is needed to better understand, on a high level, how the various solutions provide countermeasures for the security vulnerabilities present in CIM systems. It is also useful in helping to identify new vulnerabilities introduced by these systems. The next section reviews each of the four EIM architectures listed in Table 1 in more detail.

EIM Architectures

Gateway Policy Enforcement with CIM.

Gateway policy enforcement solutions represent the simplest type of EIM in terms of architecture. These solutions add a local centralized control function, enabling companies to regulate or block usage of existing CIM services. Software is installed just behind the corporate firewall to monitor all

---

**TABLE 1** Major EIM Solutions Grouped by Architecture Type

<table>
<thead>
<tr>
<th>EIM Architecture</th>
<th>Product Name</th>
<th>Vendor/Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway policy enforcement with CIM</td>
<td>Akonix L7 Enterprise</td>
<td>Akonix Systems</td>
</tr>
<tr>
<td></td>
<td>IM-Policy Manager</td>
<td>IM-Age Software</td>
</tr>
<tr>
<td></td>
<td>IM Director</td>
<td>FaceTime Communications</td>
</tr>
<tr>
<td></td>
<td>IM Sentry</td>
<td>e-Vantage Solutions</td>
</tr>
<tr>
<td></td>
<td>IMLogic IM Manager</td>
<td>IMlogic</td>
</tr>
<tr>
<td>Dedicated EIM</td>
<td>IBM Lotus Sametime</td>
<td>IBM Systems</td>
</tr>
<tr>
<td></td>
<td>Sigaba Secure Instant</td>
<td>Sigaba</td>
</tr>
<tr>
<td></td>
<td>Messaging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Professional Online</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Desktop (POD)</td>
<td></td>
</tr>
<tr>
<td>Hybrid solution</td>
<td>AOL Enterprise Gateway</td>
<td>America Online</td>
</tr>
<tr>
<td>Centralized IM control</td>
<td>Yahoo! Business Messenger</td>
<td>Yahoo!</td>
</tr>
</tbody>
</table>

---
network traffic to ensure that all CIM traffic is routed through the gateway. The gateway software then enforces specific corporate policies regarding CIM usage. Corporate policy enforcement can include blocking of some or all CIM services, blocking of some or all CIM users, and logging of conversations for regulatory compliance. Advanced features of gateway policy enforcement solutions include content inspection, auditing, and alert functions.

The key difference between gateway policy enforcement solutions and other EIM solutions is that the former primarily consists of an additional component grafted onto existing CIM networks (Figure 2). The basic functions of a CIM network (e.g., authentication, presence awareness, message routing) are neither replaced nor modified in gateway policy enforcement solutions. Rather, the core value of these solutions is the movement of administrative control of CIM use from the individual user to a centralized administrative function where corporate policies can be enforced. Although gateway policy enforcement solutions add many features to support more secure messaging in the enterprise, we say that these solutions support only CIM messaging sessions, and not EIM messaging sessions. Only CIM messaging sessions are supported because session management and message routing functions are handled by CIM services.

**Dedicated EIM.** Unlike gateway policy enforcement solutions, dedicated EIM solutions do not rely on existing CIM services networks to support real-time messaging and presence awareness functions. This architecture is independent of instant messaging networks that are installed and reside behind the corporate firewall. They are designed to mimic the functionality made popular by CIM services, but to do so more securely. All functions of the EIM network (e.g., authentication, presence awareness, message routing) are handled within the company firewall for increased security.

Because messages in a dedicated EIM solution are untouched by CIM service components, we say that this architecture supports only EIM messaging sessions and not CIM messaging sessions (Figure 3).
Hybrid Solution. Hybrid EIM solutions represent a combination of dedicated EIM and gateway policy enforcement architectures, to support both CIM and EIM messaging sessions (Figure 4). Messages between users on the same internal EIM network are routed locally (not exposed to the public Internet). Lotus Sametime includes an optional component (Sametime IM Gateway) enabling encrypted communication with external trusted partners that use Sametime software (over the public Internet).

Centralized IM Control. Centralized IM control uses a centralized hub model to support both CIM and EIM messaging sessions (Figure 5). Yahoo! Business Messenger is the only known provider of this type of service architecture, and is therefore the model used for this architecture description. In this model, message routing for both EIM and CIM messaging occurs from centrally managed Yahoo! servers. Some service functions (authentication and security management) are handled on servers inside the company firewall while other functions (presence and message routing) are handled remotely outside the company firewall.

EIM Architecture Comparison
All four EIM architectures share some level of local administrative control (Table 2). Local administrative control is the chief differentiator between EIM systems and unregulated CIM systems, in that EIM systems shift application administration responsibilities from the employee to the system administration function of the company. This shift in responsibility provides...
companies with the ability to enforce security policies regarding instant messaging use, assuming these security policies have been defined. If no security policies have been defined, or if policies have been defined poorly, the system will not live up to its implied benefits.

**Access Control.** Local access control policy enforcement is a primary selling point for EIM solutions. All of the EIM solutions examined allow local administrators to restrict access to instant messaging clients on the enterprise or employee level. Some EIM solutions allow client access control to be defined on the group level as well. Most of the EIM solutions allow local administrators to control who is allowed to share messages with whom. Different solutions support different levels of granularity in terms of what specific application features, such as file sharing, can be turned on or off. All of the EIM solutions examined allow local administrators to control whether file transfer is permitted enterprisewide, although some allow application feature settings to be controlled on the user and group levels as well.

**Authentication.** All EIM architectures, except for gateway policy enforcement, authenticate users locally, behind the company firewall. Local authentication increases security by eliminating the possibility of an attacker intercepting transmitted authentication information using a network sniffer targeting public networks.

In the gateway policy enforcement architecture, authentication messaging is routed through the gateway server to the centralized CIM authentication service. Although enforced gateway routing allows companies to restrict which users on the local area network can authenticate to the CIM service, the actual information used for authentication (i.e., screen name and password) still must be transmitted over the public network to authenticate individual users.
authentication introduces additional risk exposure.

A standard feature in most EIM solutions is the ability for companies to leverage their existing security infrastructure (specifically, corporate directory services) in authenticating employees. Corporate namespace enforcement of employee’s screen names is also widely supported. Corporate namespace enforcement provides a value-added identity verification benefit for messaging between employees. The AOL Enterprise Gateway solution, for example, provides an option Private Domain Service that allows companies to create private domain namespaces that match their existing corporate namespace, thus allowing employees to authenticate using their work e-mail addresses. Thus if Alice’s e-mail address and AOL Enterprise Gateway screen name is alice@company.com and she receives a conversation initiation request from bob@company.com, she can at least be assured that the message is coming from an authorized employee within the company.
Messaging Sessions Supported. The key difference between the four architectures presented in this article has to do with what types of messaging sessions are supported and how these sessions are handled. Gateway policy enforcement solutions support only CIM messaging sessions, whereas dedicated EIM solutions support only EIM messaging sessions. Hybrid and managed centralized EIM solutions support both types of messaging sessions, but do so differently.

If one takes as a given that CIM messaging sessions are inherently more insecure than EIM messaging sessions, then one would conclude that hybrid and centralized IM control are less secure if CIM messaging sessions are also supported. There are business reasons for why an EIM service provider would offer CIM messaging support.15 Many companies want to allow their employees to share messages with external users already on a popular CIM network. Interoperability with an incredibly large “installed base” of CIM users is compelling. However, if secure messaging is the primary motivation for using an EIM solution, companies would be better to turn off CIM messaging support if it is an option.

Message Routing. Message routing is another key differentiator among the four EIM architectures. Gateway policy enforcement solutions rely on existing centralized CIM servers for message routing. Dedicated EIM solutions add additional security by routing all messages internally, behind the company firewall. Hybrid solutions support both external centralized CIM message routing (assuming external CIM messaging is turned on) and the more secure internal EIM message routing. Centralized IM control solutions support external centralized CIM message routing and external EIM message routing. The difference between the two is that the EIM messaging channel is encrypted and can be more closely monitored for intrusions.

From a high-level architecture perspective, centralized message routing architectures do not suffer from the support redundancy of distributed message routing architectures. In theory, it should be easier, and cheaper, to maintain a centralized message routing system supporting 1000 companies than it is to maintain 1000 separate, locally installed message routing systems. It is clear that reduced total cost of ownership

<table>
<thead>
<tr>
<th>Access control</th>
<th>Gateway Policy Enforcement with CIM</th>
<th>Dedicated EIM</th>
<th>Hybrid Solution</th>
<th>Centralized IM Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Local</td>
<td>Local</td>
<td>Local</td>
<td>Local</td>
</tr>
<tr>
<td>Messaging sessions supported</td>
<td>Remote</td>
<td>Local EIM</td>
<td>Local EIM and CIM</td>
<td>Local EIM and CIM</td>
</tr>
<tr>
<td>Message routing</td>
<td>CIM only</td>
<td>Centralized CIM</td>
<td>Local EIM and centralized CIM</td>
<td>Centralized CIM and centralized CIM</td>
</tr>
<tr>
<td>Encryption</td>
<td>Depends on vendor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client software</td>
<td>Existing CIM</td>
<td>New EIM client</td>
<td>New EIM client</td>
<td>New EIM client</td>
</tr>
<tr>
<td>Interoperability with CIM</td>
<td>All major CIM services</td>
<td>No</td>
<td>Depends on vendor</td>
<td>Depends on vendor</td>
</tr>
<tr>
<td>Performance</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
(TCO) is a chief selling point for the Yahoo! Business Messenger managed solution.\textsuperscript{16}

\textbf{Client Software.} A key selling point of gateway policy enforcement solutions is that they can be installed transparently from the end-user perspective. These solutions typically use existing client application software, translating to minimal disruption to users during the switchover to an EIM solution. The other three EIM architectures require installation of new client desktop software to enable support of new EIM features. Additionally, new client software is typically needed to support message encryption.

\textbf{Encryption.} Support for confidential message transfer via encryption is a standard option for all EIM solutions, except for those with gateway policy enforcement architectures. The reason why encryption is more difficult to implement for these solutions is that existing CIM software clients do not natively support encryption. One notable exception is the IM-Age IM-Policy Manager product (http://www.im-age.com/_product/policy.html), which provides specialized add-on software for supporting encrypted messaging. Encryption helps reduce the threat of eavesdropping.

\textbf{Interoperability with Existing CIM.} All EIM architectures, except for dedicated EIM, support interoperability with CIM networks. In the case of gateway policy enforcement solutions, support for CIM messaging is a requirement. For hybrid and centralized IM control solutions, support for CIM messaging is an optional feature enabled or disabled by the local corporate administrator. As mentioned previously, from a security standpoint, interoperability with CIM is not desirable.

\textbf{Performance.} Although not strictly a security issue, systems performance is an important metric when evaluating competing systems. Performance is especially important for instant messaging applications because communications are expected to occur in “real-time.” Based strictly on architectural considerations, one can argue that architectures that make use of local message routing (e.g., dedicated and hybrid EIM) should outperform those architectures that require external message routing on the public Internet. Hybrid architecture performance depends on the messaging sessions supported. In a hybrid system, EIM messages are routed internally and therefore should outperform CIM messaging sessions in which messages are routed externally on the public Internet.

\textbf{DISCUSSION}

EIM vendors and service providers have benefited from recent industry regulations and policies requiring the recording and archiving of employee instant messaging conversations. To respond to this need, vendors have added logging and archiving features to their EIM solutions. These functions have become a primary selling point of EIM solutions as companies scramble to achieve compliance. Unfortunately, corporate instant messaging conversation archives represent an incredibly attractive attack opportunity. If these archives are compromised, the damage to the company could be enormous.

Usually, EIM solutions are more secure than CIM systems in a workplace context because the former enables the enforcement of corporate security policies, whereas the latter does not. However, the benefit of centralized local administrative control has its downside. If the company EIM administrator account is compromised, the extent of the damage to the company can be enormous. Compare this with the damage exposure in the case where an individual employee’s CIM account is compromised. Of course, one hopes that the EIM administrator’s account is more securely protected.

The comparative analysis of EIM security features reveals many approaches for securing instant messaging. The comparative analysis of architectures reveals that some approaches compromise security to support extended functionality or service
Some feature requirements exist at the expense of security and should be avoided if at all possible if high security is a priority.

business needs. Examples of extended features that compromise security include CIM interoperability, file-sharing functionality, and external messaging. A high-security IM system would avoid security compromises. Based on the comparative analysis one can extract a core set of security-prioritized features, aligned with the previously defined scenario requirements, that would form the basis of a high-security IM system.

The EIM architecture examined that satisfies the core security requirements best is the dedicated EIM architecture. Dedicated EIM solutions support these features with high performance and few points of failure. Another benefit of this architecture is that all internal communications are contained within the local area network, thus reducing the overall risk exposure of the system. Additionally, the lack of interoperability with existing CIM services is a huge bonus from a security point of view.

CONCLUSION

This article focused on security issues related to instant messaging. We first examined the threats and available countermeasures present in existing CIM services. These included viruses and worms, Trojan horses, identity theft, impersonation, eavesdropping, data loss, and denial-of-service attacks. Next we examined the variety of EIM solutions available. Following this market analysis, we considered these four classes of solutions in terms of their access control, authentication, messaging sessions supported, message routing, encryption, client software, interoperability with CIM, and performance.

The currently dominant approach to securing instant messaging communications is to shift security responsibilities from the individual user to administrators who can enforce organizational security policies. This approach is sound and consistent with how many modern information systems are secured. EIM vendors and service providers accomplish the shift in several ways. This article examined and compared four distinct architectural approaches to securing instant messaging. Different architectures optimize for different feature requirements. Some feature requirements, most notably CIM interoperability, exist at the expense of security and should be avoided if at all possible if high security is a priority. The shift of security responsibilities to organizational administration greatly increases the importance of sound security policies. The challenge for organizations will be to understand the potential threats of instant messaging and to develop enforceable security policies to counteract these threats.

References


### Additional Reading
