Systems and Network Analysis Center
Information Assurance Directorate

Secure Instant Messaging

Instant Messaging: providing secure, real-time battlefield interaction.

Maturing from commercially successful social networking origins, instant messaging (IM) technology has taken its place as a primary mechanism for information sharing in government and military organizations. Unlike their social predecessors, IM applications serving in the DoD and IC arena must provide significant security assurances and be easily managed by central administrative authorities rather than the individual users. Driven by this need for secure, multi-site and often global interactions, a variety of IM protocols and applications have emerged to fill this need.

This document provides guidance as to what capabilities should be considered vital to any organization planning to implement an IM collaboration solution. The recommendations provided are not related to any single or group of IM technologies or applications. However, similarities in architecture and capabilities give the recommendations contained herein relevance to nearly any deployment.

What capabilities are essential to providing a secure instant messaging deployment?

Amongst the wide variety of instant messaging applications available, an equally varied number of features exist within these applications. When considering which IM solution to use, the capabilities listed below should be strongly considered prior to selection.

- **Communication stream encryption**

In order to ensure the data stream is not subject to tampering or eavesdropping, encryption provided by Transport Layer Security (TLS) or Secure Socket Layer (SSL) should be mandatory. Additionally, this restriction should be enforceable by configuration of the server policy and should not rely on the client to choose to use an encrypted connection to the server.

- **Strong user authentication**

Some messaging software allows users to self-register prior to participation. This process often provides little to no authentication of the user. Others implement a better practice by requiring administrators to create accounts for each user desiring system access. This can, however, create an additional burden on already over-tasked administrators.

The best solutions allow for interaction with an organization's existing user authentication infrastructure (eg: Active Directory, LDAP, etc.) in a secure manner. Benefits to such systems include both reduced administrator workload and a lessened necessity for users to remember additional account credentials.

- **Prevention of interaction with external and undesirable IM applications**

Many users maintain instant messaging accounts with a variety of commercial providers. Enterprise IM technologies often provide the ability to serve as a bridge to these external providers, thereby consolidating the user's messaging experience. This, however, introduces a significant amount of risk into the system. Leakage of sensitive data to participants outside of the organization, the spread of malicious content such as viruses and malware, and the additional exposure of internal networks to external environments are all potential concerns.

Another possible threat is the use of unapproved or "rogue" client software. Users may intentionally introduce unapproved applications to circumvent security policy, or they may simply be seeking a user interface with which they are more familiar. In any event, steps should be taken to limit the potential for introduction of vulnerabilities.

Limiting such interactions can be accomplished via a variety of policies and settings. Capabilities which may be included in one or more server/client instantiation are:

- Client and server locking via a shared secret.

  In such systems, the server accepts connections only from those machines with knowledge of the secret.

- Disabling inbound and outbound connections on known ports used by commercial products or translation to their protocols.

  Commercial IM applications often use published ports for communication and their own proprietary protocols. By blocking communication on these ports and disabling translation to the appropriate protocols, use of these applications can be severely hindered.

- Authentication between client and server using certificate or other authentication mechanism.

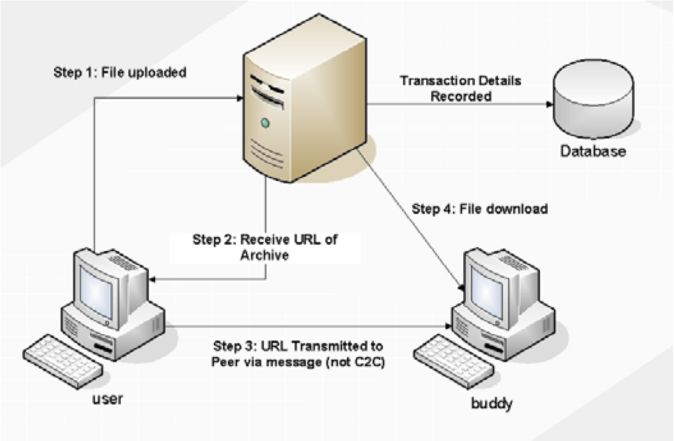
- **Platform independence**

Depending on the existing infrastructure of each organization, the operating systems on which client and server software are capable of running will influence the selection of an IM solution. While this does not directly impact on system security, consideration should be given to ensuring selected applications are cross-platform capable to provide for future scalability and network architecture modifications.

- **File sharing policy enforcement**

File sharing has traditionally introduced the most risk to IM applications. Malicious content can be rapidly passed amongst users and quickly propagate throughout a network. Although user education is essential, dedicated file transfer security capabilities should be introduced into the system.

File transfers should never be permitted between clients via direct client-to-client or “out of band” connections. Instead, the infrastructure should allow only for the passing of files via a central file transfer handler associated with the IM server. There virus scanning, logging, and quarantining of malicious files can occur.


Step 1: File uploaded
Transaction Details Recorded
Database
Step 4: File download
Step 2: Receive URL of Archive
Step 3: URL Transmitted to Peer via message (not C2C)
user
buddy

An example file sharing infrastructure

- **Central administration and logging**

The ability to administer messaging deployments from a central location and to monitor system activity is not only in keeping with sound administrative practices, but is also often mandated by organizational policy.

Administrators should be able to manage users, security settings, review logs and messages, and enable/disable the entire system by accessing only the server(s). Logging should be robust enough to link messages to individual users with appropriate date/time information in the event such information is required.

Well designed administrator interfaces will also reduce the level of technical expertise required and the possibility for errors in performing administrative tasks.

Conclusions

Instant messaging provides an immense capability to allow users to collaborate. Leveraging synchronous communications, whether they occur between the battlefield and flag staff or within the same office workspace, is essential to advancing the state of military effectiveness.

These technologies and the benefits they bring must, however, be implemented with security concerns at the forefront to prevent widespread compromises and possible hindrance of the nation’s warfighting ability. Awareness of the potential pitfalls presented here, can prevent this from occurring.