Cover Page for Paper Submission

Submission of paper for the "7th International Command and Control Research Symposium"

Topic: Multinational Information Sharing, Coalition Interoperability, C2 Experimentation,

Title of Paper: Collaboration Across the Coalition/US Only Security Boundary in the Advanced Process and Technology Experiment (APTX) 01

Authors: Stephen R. Jones and George P. Parton

Point of Contact: Stephen R. Jones

Organization: The MITRE Corporation

Address: The MITRE Corporation
202 Burlington Road, Mailstop K320
Bedford, MA 01730

Telephone: 781-271-2517

Fax: 781-271-2423

E-mail srjones@mitre.org

Collaboration Across the Coalition/US Only Security Boundary in the Advanced Process and Technology Experiment (APTX) 01

Stephen Jones and George Parton
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
(781) 271-2107
srjones@mitre.org gpp@mitre.org

Abstract

This paper presents results of a research project aimed at introducing an Instant Messaging (IM) tool across a simulated Coalition/US Only security boundary. A prototype, the Open Source Instant Messaging (OSIM) system, based on previous work in fielding collaborative systems in Air Operation Centers (AOC), was developed and fielded for the Advanced Process and Technology eXperiment (APTX). This paper will detail the motivation for creating this system, the ensuing architecture, and results from the APTX experiment. Additionally, revision requests will be examined to detail future capabilities of OSIM.

1. Introduction

For decades, and particularly since the end of the Cold War, air operations in wartime as well as operations other than war have been conducted by coalitions of nations. Command and Control (C2) of air operations in a coalition environment presents special challenges for all the participant nations and their air components. Recently the US Air Force has embarked on a series of experiments aimed at improving the way it deploys personnel and systems to support command and control. These experiments are named Joint Expeditionary Forces eXperiment (JEFX) and have been conducted in 1998, 1999 and 2000. As the early growing pains have subsided attention has focused on the importance of supporting coalition Command and Control.

In support of JEFX 02 and to provide a forum for experimentation and risk reduction, an Advanced Process and Technology eXperiment (APTX) was conducted in 2001. The central focus of APTX 01 was to confront the technical challenges of participating in the Command and Control of coalition air operations realizing that the members of the coalition would probably be unknown in advance and would differ from one expedition to the next.

The conditions set for this first experiment were less than realistic but provided developers and security agencies a place to meet and confront the first tier issues. For this mini experiment the Combined Air Operations Center (CAOC) was divided into two enclaves, a US enclave and a "Coalition Open Floor". The Coalition Open Floor would be treated as the common ground where all coalition partners who would work together to manage the air campaign. Although not simulated, it was supposed that other nations would have their separate enclaves similar to the

US enclave. The challenge of APTX 01 was to develop and demonstrate as much interoperability as possible between the US enclave and the Coalition Open Floor enclave in preparation for JEFX 02 when the bulk of the mock air war will be conducted at the coalition level.

The networks of the US enclave would be separated from the Coalition Open Floor network. Devices called *guards* were to be used to bridge the gap between networks. Such devices are presently accredited for use between individual nation enclaves and coalition shared enclaves. This involves accreditation and certification by both the individual nation and the security agency set up to represent the coalition as a body, much as NATO security would represent the combined interests in a purely NATO coalition.

A weakness of this multi-enclave environment is coordinating activities between individuals located on either side of the security boundary. Prior to APTX the extent of collaboration across any guard was supported by email messages that were assembled on a trusted email client, routed through a secondary releasing authority, and transmitted through a series of policy filters. Finally, the authenticated message would be passed to a system that could transfer the content across the security boundary. This process works in both directions with the policy filters on each side under the control and direction of the appropriate security authorities.

Email is a valid collaborative tool and in this case the default tool. The drawback with email is its latency. When secondary release individuals and the policy filters are added to an already slow process, email becomes useless for anything resembling real time communications. This process works well when operations or intelligence data needs to be passed between enclaves, but something faster, simpler to use, and secure was required to enable communications required for process coordination.

The development team’s goal was to provide a tool to support rapid collaboration and coordination of procedures and processes. Other existing systems exist to filter and pass data having operational and intelligence content. Instant messaging seemed ideally suited to supporting the collaboration and coordination needs of operators whether communicating with users in their own enclave or across the boundary in another enclave.

2. Requirements

Most companies create a productive work environment by collocating workers within a single physical location. Besides making it easier to manage people, this structure allows workers to create social networks. Team lunches, golf leagues, and water-cooler chats bring people together, creating more effective teams. Studies have shown that informal interactions support joint problem solving, coordination, mutual trust, and social learning. [Whittaker *et al.*, 1994] [Nardi *et al.*, 2000] Together these capabilities allow teams to perform tasks requiring complex collaborations.

Because of the distributed nature of coalition operations, physical collocation is often not possible. The need to keep certain information within an enclave creates a divide not only in the physical sense, but also among team members required to collaborate. A feeling of “us vs. them” can develop, hindering effective collaboration. So how can team members in a coalition environment be brought together using informal communications?

An obvious choice, especially during this age of Internet communications, is Instant Messaging (IM). IM provides a means for individuals to exchange messages rapidly with one another. Additionally, IM provides presence cues that allow a user to maintain a continual view of who is available. These features allow individuals to stay in contact with one another, even when in physically disparate locations. This is especially important among members of a team; they want to be able to maintain a sense of connection and to share in the successes of the team [Vaughn-Nichols, 2000].

IM supports several communications tasks that teams require: quick questions and clarifications, coordination of work, scheduling, organizing impromptu meetings, and simply keeping in touch with other members [Nardi *et al*., 2000]. Although other means of text communications (e.g. Internet Relay Chat (IRC), email messages, and message boards) support some of these tasks, IM has several distinct advantages. First, it provides an immediacy to its users. Individuals can easily tell who is available to communicate, and most interactions can take place very quickly. This capability can be configured through the use of “buddy lists”, which allow each user to view at a glance individuals available to chat. Additionally, IM has become very pervasive within the Internet culture. An estimated 60 million people use IM regularly, sending approximately 900 million messages on an average day [LaGesse, 2001]. And with IM making inroads into many business environments, this number will likely increase dramatically.

Another advantage of IM is that it provides a very non-obtrusive means of carrying on a conversation. In general, IM doesn’t interrupt a user’s workflow the way a phone call does [Vaughn-Nichols, 2000]. Most IM users can carry on conversations with several individuals simultaneously, but at times that are convenient to them. This is especially important for operators in a C2 environment. They can continue uninterrupted on their assigned tasks, initiating or continuing IM sessions at appropriate times. Even with this compromise on the immediacy of the tool, most users seem to feel IM offers a more responsive solution than e-mail [Vaughn-Nichols, 2000]. Additionally, IM provides a lightweight means to negotiate availability. Many users will begin a conversation with something like “are you available to talk now?” to ensure the other party isn’t busy at that particular time. When available, the other user will reply to the initial query and begin a chat session. Experienced Instant Messaging users recognize that messages may not be answered immediately, but when a buddy is ready to carry on a conversation.

Finally, Instant Messaging tools are simple to use and fit well onto an operator’s workstation. Because of the large population of users having experience with IM tools through Internet communications, the use of the tool becomes very intuitive even to a novice. The concepts of buddies and buddy lists translate universally, and make training very easy. And with the small screen footprint IM tools present, they usually fit well on a desktop with other applications, allowing operators to track conversations or availability of others peripherally, while focusing most of their attention to the tasks at hand.

However, IM systems have some drawbacks, most notably in the area of security. Many of the popular Instant Messaging systems today, including those fielded by AOL, MSN, and Yahoo, have a centralized server on the Internet that brokers interactions between users. Not only can messages be intercepted and read by almost anyone, but also IM systems with file transfer capabilities could potentially expose sensitive material to compromise. Additionally, since most coalition operations would involve networks without Internet access, what was required in this case was a complete IM system that could be contained within a secure environment.

3. Approach

Two main factors were decisive in choosing an Instant Messaging tool to field. First, it must be wholly self-contained. Because Internet connectivity was not possible during the experiment, the IM solution chosen must include a server that could be installed on both sides of the security boundary. Secondly, full access to the source code of the system was required. Because it was known early in the process that numerous code modifications would be necessary, full source code access was deemed essential. Finally, though not a priority from the beginning, having a very distributed IM system was also desired. Because the system would support two enclaves of users, the system shouldn’t encounter severe failure on one side because of the lack of connectivity between the enclaves.

Fortunately, we had a tool that met these prerequisites. The Simple Instant Messaging and Presence (SIMP) protocol, was designed by The MITRE Corporation and had included with its specification a reference implementation [SIMP, 2002]. Drafted originally as a proposed specification for the IETF’s Instant Messaging and Presence Protocol (IMPP) working group, SIMP provides much of the functionality of standard IM services. Users can initiate chat conversations in a manner similar to most other IM tools, and the presence service offered by SIMP provides functionality comparable to buddy lists. Available as an Open Source project, not only was the source code available, but expertise from the original developers could be leveraged to help field a cross-boundary IM solution.

The next piece required for an IM tool was a system that could pass information across a computer network security boundary. These systems, or *guards,* monitor information crossing network boundaries to ensure that sensitive information does not inadvertently pass from one side to another. Although a guard could be built specifically to support IM, this would require a great deal of time and effort not only to create, but also to obtain accreditation from security authorities to operate on a secure network. For this particular experiment, it was felt that using an approved guard system would greatly lessen the risk of fielding a cross-boundary IM system. The guard would handle the transfer of information across the boundary in an appropriate manner, freeing the developers to concentrate on providing the capabilities of Instant Messaging. Although the Information Support Server Environment (ISSE) guard [ISSE, 2002] was used for this experiment, it is felt that any approved guard system that accepts formatted messages could be used within this IM architecture.

3.1 *Server Architecture*

A significant advantage SIMP has over many of the other IM systems is that it implements a very distributed architecture. It does not rely on a centralized server to coordinate users, but instead supports a network of several servers that together form the IM system. Figure 1 illustrates an example SIMP network. SIMP servers provide a connection point for users within their local domain, while servicing presence and messaging requests from other servers. This provides users a seamless IM system that can scale to a very large number of users.

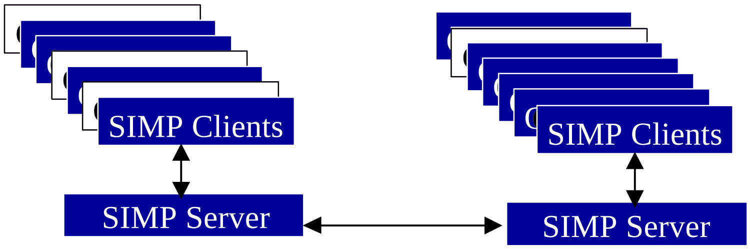


Figure 1 – SIMP Architecture

The Open Source Instant Messaging (OSIM) system builds off of the distributed architecture of SIMP. Because there will be two or more distinct networks, it becomes a logical first step to install an OSIM server to control IM within each enclave. These servers can be managed by the administrators of their respective enclaves, allowing those administrators to control their users as necessary. To enable cross boundary communications, the ability to transfer the server-to-server messages is required.

In examining the server-to-server communications specified by the SIMP protocol, 6 messages were deemed essential. These include the *Send* message for text communications, the *Describe*, *Change*, *Subscribe*, and *Unsubscribe* messages to support presence awareness, and the *Acknowledge/Error* message to provide response feedback. These messages are formatted using XML to allow for simple message creation and parsing. The OSIM solution needed to support these messages in order to support the capabilities provided by SIMP.

Figure 2 shows the solution designed by the OSIM development team. A new entity, the *OSIM Proxy Server*, was added to each enclave involved in the coalition. This proxy implements an interface similar to an OSIM server, but instead of applying the server logic it instead provides a message translation and forwarding capability. The Proxy accepts messages designated for a user on the other side of the enclave boundary and formats it according to the rules imposed by the guard. Once received on the other side of the boundary, the corresponding Proxy can regenerate the XML message to pass to its companion OSIM server. Although the implementation for APTX creates messages specifically for the ISSE guard system, it is felt that this Proxy design makes it easy to interface with other guard systems.

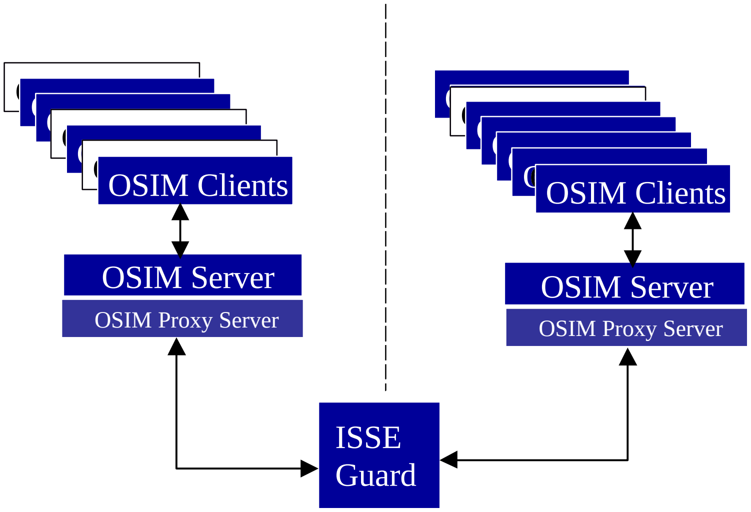


Figure 2 – OSIM Architecture

A major assumption made during the development of the OSIM system was that most users would try to follow the security guidelines and wouldn't purposely compromise sensitive information. A variety of means could be used within the capabilities of free-text chat, such as using encoding mechanisms, which would allow individuals to secretively pass information. Although this was seen as a low-risk possibility, logging capabilities were enabled in the Proxy servers. Normally discouraged in collaborative tools because they may limit the free exchange of information between users, logs are seen as a necessary precaution when information is being exchanged across security boundaries.

Another precaution put into place by OSIM was the translation of user identities to a numeric value. Because of the distributed nature of the SIMP protocol, all messages have a combination of *To* and *From* identification fields being passed as text data. Implemented in the Proxy through the use of a user translation table, this capability provided several functions. First, only users designated within the translation table could pass IM messages across the coalition boundary. This provided a means for security personnel to limit the individuals having cross boundary privileges. Also, the translation of user identities limited information about individuals being passed across the coalition boundary. Although in APTX the user translation tables were identical in both enclaves, a security manager would have the capability to create a "releasable" user list that could be passed to the other side of the security boundary.

3.2 *Client Implementation*

In designing the client, the OSIM team wanted to maintain the basic SIMP implementation on which it was based. The SIMP client provided functionality in a manner familiar to most IM users, an aspect we did not want to lose. Additionally, because of limitations on time and manpower available, a completely new client could not be created. However, the team felt interface changes were necessary to inform operators of the new collaborative environment in which they were participating. Because a cross boundary use of IM is significantly different from the way the operators will have used IM, a tailored client implementation was required.

The first change to the user interface involved a modification to the operator's buddy list. Within the OSIM system, a buddy list can include individuals from two different areas: users within the same enclave as the operator and those outside that enclave. To support this notion of two groups of users, the buddy list provides an icon to designate each. Figure 3 illustrates OSIM's implementation of these icons. Individuals with blue icons in front of their names are operators on the same network as that user. The yellow triangular icon designates operators that reside on the other network. In this example, the user is logged into the "Coalition" enclave and has two buddies online: testc3@kagoona.mitre.org residing in the same network, and testus1@harley2.mitre.org working in the "US" enclave. With these icons, users can tell at a glance where their buddies reside.

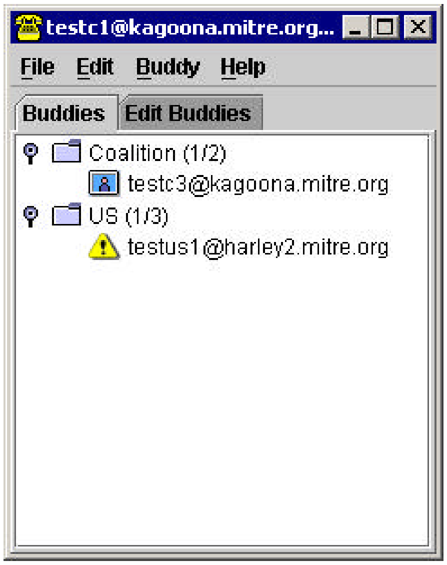
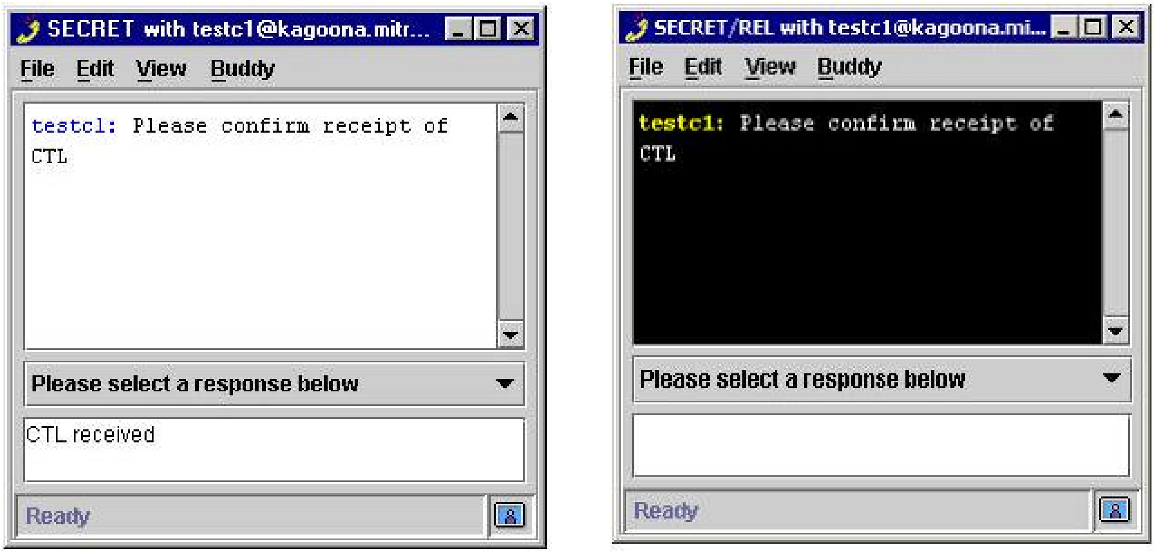


Figure 3 – OSIM Client Buddy List

From their buddy list, a user can initiate an IM session by double-clicking on a buddy's name, or from the selection on the **File** pull-down menu. Once a session is initiated, a chat window will be opened on both users' desktops. We felt that the IM session windows should provide a strong visual cue to the user indicating the security level of the other individual. Because users likely will be involved in several conversations simultaneously, they need to be continually aware of the security level of each conversation. Figure 4 shows the OSIM implementation of the session windows. Reverse-video conversation scroll-back areas provide the main visual cue to the user. Sessions with users located in the same enclave will have the standard white background and an appropriate window title, while sessions with operators in another enclave will display a black background, reversed font colors, and an appropriate window title.


SECRET with testc1@kagoona.mitr...
File Edit View Buddy
Please select a response below
Ready
SECRET/REL with testc1@kagoona.mi...
File Edit View Buddy
Please select a response below
Ready

testcl: Please confirm receipt of CTL

CTL received

testc1: Please confirm receipt of CTL

Figure 4 - Session Dialogs with users inside the same enclave (left) and with a different enclave (right)

In order to enhance the security of the system by reducing user errors, a couple of changes were also made in the way the user can send text messages. Each free text message within OSIM has a limitation of 256 characters, pasting data into the clients from other applications on the desktop is disabled, and information can't be saved from the scroll-back window. Because OSIM exchanges normally involve very short messages intended for coordination and collaboration on processes, procedures and activities, these limitations should not diminish the tool's usefulness. These limitations were put in place to deter the intentional release of sensitive information and to help keep well-intended users from making mistakes. OSIM was not designed as a replacement for the use of email or other prescribed tools for transmitting text with significant operational or intelligence content, but to assist in the coordination of collaborative activities.

4. *Results and Analysis*

During May of 2001, OSIM was fielded and participated in the APTX experiment held at Langley AFB, VA, USA. Throughout this period of time, up to 16 operators, controllers, and support personnel used OSIM to coordinate their activities within and between two separate enclaves. Although a small experiment, the OSIM development team was able to observe the use of the tool and the benefits provided to the operator. Additionally, a small survey was conducted to help discern the effectiveness of the tool as implemented.

Our first observations were that the tool's intuitive IM interface allowed users to quickly learn the use of the tool. An informal training session was held before the beginning of the experiment to introduce OSIM to the operators and point out differences between it and other IM tools. Apart from adding users to one's buddy list, which did not follow other well-known IM tool interfaces, users were able to easily determine presence of other users and start chat conversations. Most became enthusiastic users because of the ease of use and started several chat sessions within a short period of time.

Because the tool was easy to use, it quickly became part of many users' work activities. Even though the operators' tasks were scripted through a large part of the experiment, OSIM played a significant role. This was especially true for the experiment controllers, who had their choice of tools to coordinate scenarios. They found OSIM provided a simple, unobtrusive means to keep both enclaves informed of the scenario being executed. Experiment assessors also found OSIM useful as they could coordinate activities whenever convenient. They also found the time-stamping feature of the messages helpful; this allowed the session windows to become a "diary" from which they could review activities at a later time.

What the tool also allowed was the spontaneous, social interactions not normally found in a collaborative environment such as this. Although the operators also had Voice over IP (VoIP) phones available to them, they found that OSIM allowed them to carry on personal conversations. Topics such as where people had dinner, what was on television, and even Professional Wrestling were observed. These kinds of interactions have the effect of bringing a coalition team together, even while individuals reside in different locations.

A weakness in the OSIM system noted during the APTX experiment was the performance of the interactions across the ISSE guard. Having text, presence, and associated response messages crossing the enclave boundary combined to slow performance considerably. Although some internal configuring of both the guard and OSIM system allowed for reasonable operations, the development team felt that the system as fielded would not scale to a larger JEFX experiment. A main priority taken from the APTX experiment was to address this issue.

To judge the effectiveness of the user interface changes made to the OSIM client a simple survey was conducted by the assessment team. Tables 1 and 2 show the results of this survey. Although the target audience was a small group, some observations became apparent. First, the changes made to the client seem to be informative to the majority of the users. For both questions, most of the operators were aware of the changes made to the client interface. However, both questions also showed that the changes were not completely understood by everyone. We view this as mostly a training issue; these individuals may have missed the training at the beginning of the experiment, or hadn't grasped the concepts when presented. Because most users easily understood the operation of the tool, more time could be spent emphasizing the visual cues indicating cross boundary collaborative sessions.

Table 1 - Do the two different icons help you tell the difference between buddies within the enclave and those across the coalition boundary?

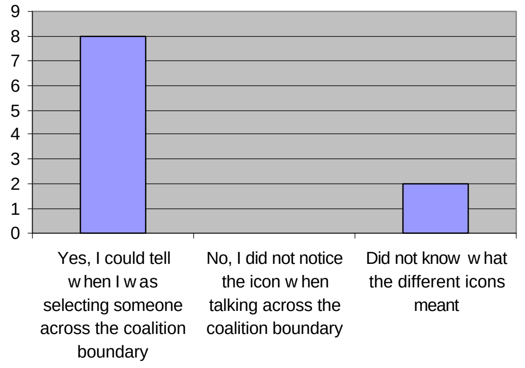
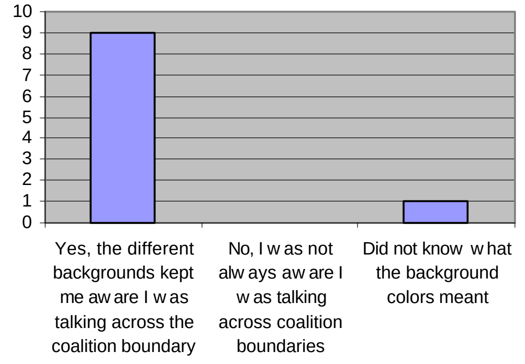


Table 2 - Do the different backgrounds for the chat windows help you remember when you are chatting across the coalition boundary?



5. Future Work

Because the APTX fielding of the OSIM system was the initial prototype, many improvements could be made. Feedback received from operators, and observations made by the design team provided several areas of improvement. We hope to implement many of these ideas with the next prototype, which possibly could be fielded for use in JEFX 02.

The first area to be researched will be performance issues between OSIM and the guard system. Because a relatively small number of users had a significant impact on the responsiveness of the cross boundary system, this area will be a very high priority. Much of this work will include coordinating activities with guard developers to make the transfer of IM messages as efficient as possible and will likely require changes to both systems. Additionally, because the ISSE guard used during APTX handled message traffic other than OSIM, prototypes with dedicated guard systems should be tested. Finally, operating with a secondary guard installed to perform load balancing should be prototyped.

From speaking with operators during the APTX experiment, a highly requested feature enhancement was the addition of group chat. During the experiment, it wasn't uncommon for an operator to have 3 or 4 chat windows open simultaneously, carrying on a similar conversation. Work has begun on modifying the protocol to support group communications. However, the required changes to the user interface will raise some interesting questions. How will a group of individuals from different enclaves be displayed? Could only certain individuals within the group have chat directed to them when necessary? Does group chat present problems in maintaining the context of a conversation? These questions will need to be addressed as the prototype develops.

In addition to some known client problems, one major improvement to the security of the system would be the addition of digital signatures. The APTX experiment did not have a PKI infrastructure in place, so the use of signatures was not a possibility. If a certificate authority is fielded in JEFX 02, then signatures could be added to messages being sent, improving their authenticity. The disparate nature of a coalition architecture makes client-to-client validation unlikely, however messages could be signed and verified as they move from point-to-point through the system.

Long range plans for the OSIM system could include integration with other collaboration tools. One prototype developed as a research project within MITRE ties an Instant Messaging system with language translation capabilities. Although allowing mixed nationalities to now communicate in their own language, user interactions with IM would need to be examined more closely. Users can not type as quickly as they speak, so often these users will use language shortcuts or slang as normal conversation. Since common language translation tools handle slang poorly, these language idiosyncrasies will need to be examined more closely when used in conjunction with IM. Another possible collaborative tool integration could be tying in VoIP capabilities with IM. Several major IM services have begun integrating audio and voice with their chat services already, allowing users to move to a richer means of communication as required. Since a prototype VoIP capability was demonstrated during the APTX experiment, bringing these two technologies together seems to be a possibility in the future.

6. Conclusion

The OSIM system as fielded at the APTX experiment provided a level of informal communications not experienced previously in a CAOC environment. While phone networks and email messages allow for the transfer of information between enclaves separated by a security boundary, coalition members existed as disparate groups. Operators residing in one enclave never had the ability to create the kind of social connections with their counterparts that would allow these kinds of interactions. With OSIM, these same operators now have the ability to quickly contact each other to coordinate activities and solve problems.

The use of Instant Messaging provides an intuitive means to provide informal communications. Because so many people have a working knowledge of IM, many operators assigned to a CAOC environment will know terminology, etiquette, and the use of IM tools. During APTX, operators quickly became proficient with OSIM and were sending messages within minutes of being introduced to the tool. Processes could be controlled quite tightly, and questions such as "what are those guys doing in the other enclave?" were seldom heard.

However, the security aspects of cross boundary collaboration can't be forgotten. Potentially sensitive information could be compromised using the OSIM system. Providing visual cues and placing some restrictions on the information crossing the security boundary aids in limiting unintentional release of information. Additional emphasis on the security aspects of OSIM must be provided during training to ensure all users understand when information is being passed to another enclave. Digital signatures could be introduced to ensure the authenticity of users participating in IM.

The popularity and simplicity of IM could allow OSIM to be combined with other collaborative tools. Capabilities such as language translation, group conferencing, and audio conversations could enhance the collaboration experience for the user. Each of these enhancements need to be examined separately to ensure that they don't 1) create unacceptable security vulnerabilities, 2) unnecessarily complicate the tool, and 3) provide a capability not required by a Command and Control user.

From the fielding of the OSIM system, the benefits of informal communications were demonstrated. Users at all levels had the ability to coordinate activities at a level unseen before in this environment. Activities became easier to accomplish, and social interactions between enclaves developed. As current cross boundary tools don't provide important informal communication mechanisms, OSIM provides an important and much needed capability for a coalition environment.

7. *References*

[Whittaker *et al*., 1994] Whittaker, S., Frohlich, D., & Daly-Jones, W. (1994). Informal Workplace Communication: What is it Like and How Might We Support It? *Proceedings of CHI '94 Conference on Human Factors in Computing Systems*, 131-137, ACM Press: New York.

[Nardi *et al*., 2000] Nardi, B., Whittaker, S., & Bradner, E. (2000). Interaction and Outeraction: Instant Messaging in Action. *Proceedings of CSCW '00 Conference on Computer Supported Cooperative Work*, 79-88, ACM Press: New York.

[Vaughn-Nichols, 2000] Vaughn-Nichols, S. "Instant Messaging Goes Corporate: How IM is Working in the Workplace". Web reference: http://www.zdnet.com/sp/stories/column/0,4712,2686390,00.html.

[LaGesse, 2001] LaGesse, D. "Instant Message Phenom is, Like, Way Beyond E-mail". Web reference: http://www.usnews.com/usnews/issue/010305/nycu/im.htm.

[SIMP, 2002] SIMP Project Homepage – http://simp.mitre.org

[ISSE, 2002] ISSE Guard Program Office Homepage – http://www.rl.af.mil/tech/programs/isse