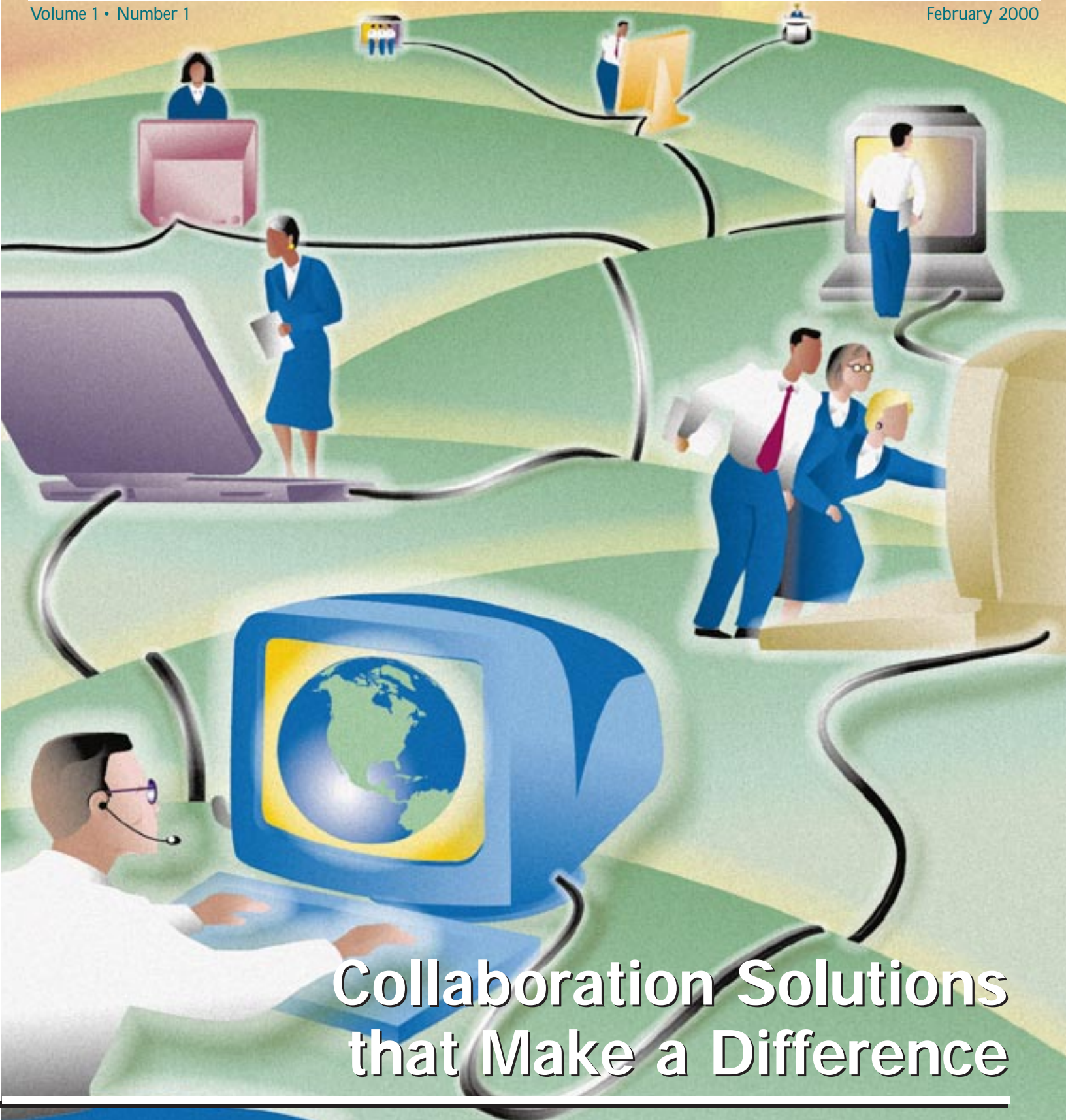


THE ***EDGE***

PERSPECTIVES

Volume 1 • Number 1

February 2000



**Collaboration Solutions
that Make a Difference**



The EDGE PERSPECTIVES
MP-990000253

The EDGE PERSPECTIVES is published by The MITRE Corporation.

© 2000
The MITRE Corporation.
All rights reserved.
This document has been approved for public release.

The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

1820 Dolley Madison Boulevard
McLean, VA 22102

www.mitre.org

Regina Hansen, Managing Editor

Francis McLoughlin, Editor

John Schleith, Art Director

Mark Maybury, Publisher

For newsletter feedback or submission information, contact:
Regina Hansen
Telephone: (703) 883-7301
E-mail: hansen@mitre.org
Mail Stop: W650



A publication of the MITRE I-Team

<http://www.mitre.org/resources/specialty/i-team/homepage/>



Welcome to *The Edge Perspectives*. *Perspectives* complements our traditional *Edge* information technology magazine by presenting objective and balanced corporate viewpoints on strategic technology areas and issues. Please let us know how we can improve *Perspectives* to better serve you.

Vic DeMarines
President and CEO
The MITRE Corporation

Message from the Publisher

This inaugural issue of *Perspectives* considers a strategic opportunity and challenge facing MITRE sponsors: How can we enable teams and organizations to collaborate effectively? MITRE is designing collaboration services for the warfighter, analyst, and policymaker that span geographic, temporal, and organizational boundaries. MITRE's vision for collaboration services includes conferencing, information sharing and place-based interaction to enable genuine process improvement. Associated cost, schedule and performance benefits are achievable in multiple domains including planning, operations, logistics, and training. As the pages herein provide testimony for, however, the most important challenge is organizational: creating a culture of collaboration through strategy, policy, and incentives. The impact can be dramatic, exemplified during 1998's Desert Fox in Iraq and last year's Kosovo operation, when the MITRE-engineered Collaborative Contingency Targeting (CCT) system (see *Edge* special issue on Collaboration, http://www.mitre.org/pubs/edge/june_98/) enabled the Cruise Missile Support Activity and theater commanders to reduce the time-lines for distributed targeting for Tomahawk Land Attack Missiles from days to hours. This issue conveys our viewpoints on the marketplace, technology transition, security, standards, and research.

We hope you enjoy our *Perspectives*,
Mark Maybury, Publisher



Inside this issue



Collaboration Marketplace Evolving to Meet Emerging Needs
Page 1

Collaboration Technology Insertion
Page 4



Balancing the Requirements of Collaboration and Security
Page 6

Challenge Problems Guide the Future of Collaboration Research
Page 8



ITU Works Toward International Telecommunications Standardization Page 3

IETF Working Group to Define Presence Information Page 7

OMG's Open Specifications to Provide Interoperability Solutions Page 9

http://www.mitre.org/pubs/edge_perspectives/

Collaboration Marketplace Evolving to Meet Emerging Needs

By Lucy Deus

The collaboration marketplace has been evolving over the last 10 years, delivering technologies that enable coordination and information sharing, virtual meetings, and more recently virtual collocation. The promise of these technologies is to improve our ability to collaborate, coordinate, and share information to facilitate inter- and intra-organizational teams. With these technologies, we have an opportunity to better support the mobile workforce and leverage personnel assets, wherever they may be.

State of the practice – Coordination & information sharing

Most organizations use asynchronous collaboration tools that enable the work force to coordinate and share information with each other. Examples include e-mail, discussion groups, information sharing tools, and group calendaring systems. These tools allow people to work together, regardless of whether team members and work products are physically collocated. Tools such as e-mail enable team members to exchange electronic messages with attached files. Discussion groups enable teams to conduct threaded discussions, which are available to the team. Information sharing tools such as Web servers and Lotus Notes enable teams to publish information and can provide an interface to share information in corporate directories and databases. Group calendaring systems enable teams to schedule meetings and the necessary resources for the meeting.

This market segment has been maturing over the last 6-10 years and provides a stable technology base, with scalability to support the enterprise. Most of these tools have support for security (e.g., authentication, encryption, and firewall support). Tools from different vendors are largely interoperable, with most



vendors conforming to common standards or exchange formats. It is quite common to find many of these complementary tools bundled together as part of a product suite. Key vendors with offerings in this area include Microsoft, Netscape, and Lotus.

State of the art – Virtual meetings & interactive production

The marketplace for real-time conferencing tools has been very active over the last 2-4 years. Real-time collaboration tools take us to the next level of collaboration and provide us with the ability to conduct virtual meetings and share information in real time. Examples include text chat, audio/video conferencing, and data conferencing (e.g., shared whiteboards, and real-time application sharing).

Text chatter has gained in popularity over the last 1-2 years with the emergence of a new class of chat tool that supports online

presence awareness in addition to the chat capability. Tools such as AOL Instant Messenger and AOL's Mirabilis ICQ (I Seek You) allow users to create tailored "buddy lists" so they can be made aware when users of interest come online and are available to chat. These tools make it very easy to conduct one-on-one or group discussions. These tools are highly scalable and require very little network bandwidth resources.

Audio and video conferencing tools have started to become more viable over the last 1-2 years, but still suffer from issues of stability and scalability to support large conferences. These tools require sufficient network bandwidth and quality of service to be effective on any scale, though users can effectively use audio on low bandwidth connections such as dial-up. Multipoint conference servers, such as those provided by Data-Beam, White Pines, Onlive, and PictureTel, are required to enable multiple users to participate in an audio/video conference. There are many audio and video conferencing tools, which are interoperable through their

Collaboration technologies are those technologies that enable people to share information, communicate, and coordinate across time and distance boundaries.

Continued on page 2



The MITRE Collaboration Team discussing the ubiquity of collaboration extending from the desktop to the palmtop.

Collaboration Marketplace

continued from page 1

support for the International Telecommunications Union ITU H.323 (see related article on page 3) conferencing standard. However, there are still proprietary vendor solutions in the marketplace that are not interoperable with other tools.

The use of data conferencing tools, especially application sharing, has become more popular in the marketplace with the free availability of Microsoft NetMeeting and similar free tools for Sun and SGI platforms. Most vendors are adopting a common implementation for real-time application sharing into their products (e.g., PictureTel, Intel, Microsoft, and Sun), based on the ITU T.128 standard. Shared whiteboard capabilities have remained constant over the last few years, and only custom solutions provide the additional capability required by the Department of Defense (DoD), such as support for geo-registration and specialized image formats (e.g., National Imagery Transmission Format). Many shared whiteboards are not interoperable with each other, and there has been a noticeable lag in adoption of common standards by the vendors. Both application sharing and shared whiteboard data conferencing tools are limited in scalability, and suitable only for smaller work teams. The ITU T.120 family of data conferencing standards, although followed in part by some vendors, has not been adopted as a whole by the vendor community. There has been recent activity in lighter weight approaches to data conferencing that are more Web friendly that will challenge the ITU T.120 standards. (See ITU article on page 3 and IETF article on page 7.)

Security has not been adequately addressed by the real-time conferencing tools. Although most chat tools support some form of authentication, they typically do not support encryption of the chat conference data, and some tools introduce firewall risks. Audio/video and data conferencing tools can introduce serious firewall risks, typically have no support for authentication, and we are only beginning to see encryption support for some data conferencing tools, as Christine Eliopoulos chronicles on page 6.

Very leading edge – Virtual collocation

The next wave of collaboration technologies emerging in the marketplace are environments that support virtual collocation, often referred to as “place-based” collaboration environments. These environments integrate people, communications, and shared data, into a shared virtual space. The environment itself is persistent, which means that the shared space, shared data, and properties of the collaboration environment do not go away (such as in a virtual meeting) and remain available to support ongoing collaboration. Some key properties of place-based collaboration environments include rich communications (e.g., text chat and audio/video conferencing), a shared document store to make documents and other data available to others, tailorable virtual spaces to provide the location and context for the collaboration, conference management for managing chat, audio/video, and other conferences within the collaboration context, and presence awareness so that users are aware of others that are available in the collaborative environment.

Place-based collaboration is still an active research area, with two commercial products available in the last two years, TeamWave Workplace and General Dynamics (formerly GTE) InfoWorkspace. Place-based collaboration environments are not yet interoperable with each other, and there are currently no standards for virtual space environments. Although the environments support authentication, and privacy of the virtual spaces via access control lists, additional security is beginning to be addressed by the vendors, with a lack of secure communications and firewall risks.

From bundled toolsets toward system frameworks

Collaboration offerings have developed in the marketplace as individual applications and as bundled toolsets that offer a tight package of complementary functionality. As demand for collaboration grows from workgroup to enterprise and cross-organizational scale, we expect commercial offerings to evolve toward a system framework approach, where collaboration services become integrated with the information infrastructure. The services-based framework, as the longer term architectural approach, will give us flexibility in product choices to satisfy user requirements, competitive advantage to benefit from rapid technology evolution and innovation, and interoperability from leveraging existing enterprise services (e.g., directory, security, document, search, workflow, and network services). Implementing such a framework is challenging and requires time, as the components for the framework become available and the techniques for integrating the services become better understood.

In the near term, the bundled toolsets will continue to be viable, providing an “out of the box” capability that can be easier to deploy and administer, but with less flexibility with interoperability and tool integration. The critical factor will be for planning for the migration from the tightly integrated toolsets toward the system

“In order for an organization to be able to successfully use collaboration technologies on an enterprise scale, the network and systems infrastructure must be able to support the requirements of the collaboration tools.”

frameworks, with understanding of life cycle costs and impact of migration on users.

Why aren't we there yet? – Implementation challenges

As the market continues to rapidly deliver collaboration offerings, organizations have yet to adopt many of these collaboration services into the enterprise. The state of the practice in most organizations is with the use of asynchronous collaboration technologies (e.g., e-mail, threaded discussion groups, Web/document servers, group calendaring). Adoption of real-time conferencing is occurring at a slower rate than initially anticipated, but is expected to grow in the next few years, with a focus on data conferencing. The Gartner Group anticipates that synchronous collaboration technologies will be in use by over 10 million users by 2002. The government is ahead of commercial industry with respect to understanding requirements for virtual collocation, and the demand from commercial industry is expected to follow.

But even in the government, there continues to be more of a focus on pilot programs and limited operational deployments rather than enterprise deployment of advanced collaboration services. Reasons for the slower adoption can be attributed to technical/infrastructure, security, and cultural issues.

In order for an organization to be able to successfully use collaboration technologies on an enterprise scale, the network and systems infrastructure must be able to support the requirements of the collaboration tools. Real-time conferencing requires available bandwidth and quality of service from the network. Some tools require support for IP multicast routing. Organizations must prepare a strategy for managing large-scale rollouts, network advances, administration, training, and support.

To enable cross-organizational collaboration, security policies and security solutions must be in place. Security is often weakly addressed by collaboration tools, requiring organizations to consider additional technologies (such as virtual private networks) and flexibility in security policy and an agreed upon concept of operations to enable collaboration across organizations. This poses a great challenge to adoption of collaboration, beyond challenges we face with technology, since there are no policies in place for supporting virtual organizations.

The most difficult challenge is that of dealing with organizational culture and organizational readiness to change to support collaborative operations. Even if the systems, networks, and security policies are in place, and the collaboration technology is the most

capable and robust, it will not have an impact if the members of the organizations do not see a need or do not have a willingness to share information and collaborate. Organizations must work within to create a collaborative culture in the organization and help members to understand the benefits and rewards, how they are expected to work, and how they will be supported. Organizations need to work with staff to understand how to use collaboration technology to improve the business process and realize improvement. Members of the organization should be involved from the beginning in helping to define the concept of operations, understanding the rollout and training process, and evolving organizational goals.

All of these challenges in implementing collaboration take time, careful planning, and come with an associated cost. Piloting and early experimentation, with a plan to build upon lessons learned and expand to more members of the organization, can help to ease the rollout process. Organizations should expect failures, but examine them closely to understand the causes, so that the next iteration can become more successful.



For more information, contact Esther Rhode at 781-271-8889 or erhode@mitre.org

ITU Works Toward International Telecommunications Standardization

By Grant Paul

The International Telecommunications Union – Telecommunications Standardization Sector (ITU-T) studies technical, operating and tariff questions and adopts recommendations on them with a view to standardizing telecommunications on a worldwide basis. One of the 14 Study Groups (SG) that make up the ITU-T is responsible for generating the recommendations for data

collaboration and videoconferencing. T.120 is a family of recommendations that define the protocols for data collaboration, and H.3xx are “umbrella” recommendations for videoconferencing. It should be noted that T.120 is “network independent,” while the videoconferencing recommendations are keyed to a particular network transport (e.g., N-ISDN, ATM, IP, etc.). Read more about the ITU Video-

conferencing and Collaboration Standards online at

http://www.mitre.org/pubs/edge_perspectives/february_00/paul.html



For more information, contact Grant Paul at 781-271-7226 or gpaul@mitre.org

Collaboration Technology Insertion

Disruptive Technologies Challenge Conventional Wisdom

By John Davidson

Over the last three years, a relatively small team working out of a Defense Department intelligence organization has built and maintained the largest online multimedia collaboration service in daily use by the United States Government. The service supports more than 3,000 users at over 50 sites around the world. This represents a tremendous success, and a significant challenge to conventional wisdom.

Conventional wisdom would have one believe that successful technology insertion must follow six hypothetical guidelines:

- The organization's culture must naturally support collaboration.
- Exhaustive requirement analysis is needed to ensure success.
- You need broad high-level management support.
- The information technology (IT) infrastructure must be accommodating.
- Build it and they will come.
- You need a lot of money to deploy collaboration technologies.

None of the above guidelines proved entirely true in our experience. The Collaborative Virtual Workspace (CVW)-based virtual communities supported by the Community-Wide Enterprise Facility (CWEF) have become extremely valuable, and this article addresses several key reasons for their success (see definitions on page 5). We offer these as lessons learned for others attempting to modernize a large organization's business practices using collaboration technologies.

Guideline 1: The organization's culture must naturally support collaboration.

Intelligence analysts have been trained to produce world-class technical intelligence products in a culture that rewards closely held ownership of information. The analytic work force is compartmentalized, with the rationale that the more segregated key aspects of a classified truth can be



Collaboration is key to building agile business processes.

made, the less likely it will become known to those without the “need to know.”

Agency downsizing has led to the loss of senior analysts and managers, and to increased “outsourcing” and decentralization of many critical functions in the production process. There is a growing awareness that working smarter, not harder, means working together, and breaking the dependence on historical linear processes (stovepipes) in favor of a non-linear and more agile business model (see illustration).

Intelligence agencies respond daily to a wide range of national security and humanitarian crises in support of national decisionmakers. We knew that if we could support crisis operations, we could gain access to the most committed analysts/managers, and enlist their help in revolutionizing the agency's business.

On balance, the community's culture of inward-looking analysis and secrecy worked against us, but we were able to leverage the agency's ability to rally in a crisis to our advantage. Once we experienced some real operational successes, we were able to keep up the momentum.

Lesson Learned: *All large organizations are feeling “market pressures” to react to a rapidly changing world, particularly the larger intelligence agencies.*

In such cultures, the need to change is a powerful ally in addressing substantive cultural barriers to collaboration, but you have to highlight the compelling business arguments supporting that change. In our case it was crisis support. Find the part of your enterprise that can leverage the technology to produce real results, and work there.

Guideline 2: Exhaustive requirements analysis is needed to ensure success.

While it is important to know what problem it is you are trying to solve with technology deployments, it is equally important not to lose sight of the ultimate goal. Because collaboration technologies are changing so rapidly, any effort at detailed requirements analysis will be quickly overcome by events. Offices insisting on having all the answers in such a dynamic environment end up endlessly studying the problem and never reaching the deployment stage.

The CWEF sought to avoid this trap because we knew we lacked the knowledge and experience to make complete judgments, and that we could only gain such knowledge through experience. We decided to take a first step with CVW, which met the basic requirements. The CWEF deployed it, formed some communities, gained some operational successes, and revisiting the tool selection decision later as needed. One can

CWEF: *The Community-Wide Enterprise Facility is a small office within the intelligence community that is focused on technology discovery, trial, and insertion. Its specific goal is to facilitate intelligence process reengineering through the successful introduction of advanced information systems technologies.*

CVW: *The MITRE-developed Collaborative Virtual Workspace is a prototype collaborative computing environment, designed to support temporally and geographically dispersed work teams. From a user's point of view, CVW provides a persistent virtual space within which applications, documents and people are directly accessible in rooms, floors, and buildings. From a technical point of view, it is a framework for integrating diverse collaborative capabilities.*

fill out the capability matrices later after one knows what the specific capabilities mean to the success of the mission.

In short, CVW was introduced not because of its innovative technology, but rather to try to break specific intelligence processing flow bottlenecks. This is a fundamental difference in approach.

By maintaining our focus on the near-term intelligence mission, everything we did with collaboration became a mission support activity. We trained users using mission scenarios, we added mission-application mime-types into the collaboration document server, we co-opted mission support resources to support the system rollout, and most of all, we defended our work on the basis of potential (and then demonstrated) benefits to the operational mission.

Lesson Learned: *It's not the technology, or the process, but rather its application that is the key to success*

Guideline 3: You need broad high-level management support.

It's good when you can get it, but the nature of collaboration systems as a disruptive technology (*The Innovator's Dilemma-When New Technologies Cause Great Firms to Fail*, Clayton M. Christensen, Harvard Business School Press, Boston, Mass., 1997) means that broad management support is probably unattainable early on. Instead, we prepared for broad opposition, and enlisted one senior manager willing to defend the effort at critical junctures.

We worked with teams willing to risk change, and focused on building mission successes. We saw senior management become converts when presented with capabilities that made a difference.

Early resistance to deploying collaboration technologies was overcome when it was realized that, out of all the software programs and networks supported, CVW was the only package in constant and urgent demand.

To address fears of network impacts, we documented network loads with CVW use and found them to be minimal. We enlisted the support of the network engineering team so that our results would be viewed as unbiased.

Lesson Learned: *The root of most management opposition is fear. You have to overcome fear with documented test results, overwhelming customer demand, persistence, and a generous supply of "get out of jail free" cards from at least one senior manager.*

Guideline 4: The IT infrastructure must be accommodating.

This is the one guideline we agree with. The agency's enterprise architecture was indeed well prepared for wide deployment of a collaboration application. The agency maintains a worldwide computing network; its users have high-quality desktop workstations, reliable networks, and they have become accustomed to this level of support. Without such an infrastructure, we would have been severely constrained.

Even so, the network infrastructure was not prepared for the IP/Multicast protocol required by CVW for its streaming audio and video channels. We took particular care to create an IP/Multicast backbone, or MBONE, on top of the physical network layer, because we knew the network infrastructure support teams could easily stop the deployment effort if it was suspected that the collaboration system posed a threat to the stability of their extensive networks.

We overlaid the MBONE on the physical network topology to maximize performance and minimize impact on other applications. We spent months researching the physical networks, working with the network modernization teams and others to make sure our MBONE would not cause unnecessary network loading. In the end, we gained the trust and respect of the network engineers who are responsible for the health of the agency networks.

Lesson Learned: *The critical aspects of any collaboration system lie in its supporting network communications technologies. If you want to fit the sys-*

tem into your enterprise structure, get a good network engineer on your team from the beginning, and make your initiative fit the infrastructure.

Guideline 5: Build it and they will come.

This argues that standing up the capability is all one need do, and that once in service, it will draw users in. This couldn't be further from the truth.

We had to build compelling business cases and publicize them to the work force through their peers in order to win over skeptics. This is organizational change in action, and it's painful. No organization changes on its own accord without a compelling reason to do so.

Rather than deploying the capability widely, we made a conscious decision to be highly selective, working only with senior analysts and managers who knew they had a need for advanced collaboration capabilities, or had exhausted all other means at their disposal (secure phones, e-mail, newsgroups, IRC chat, etc.). They were willing to participate either because they had rare foresight or because they had a mission to perform that could not be supported by traditional means.

This process became enshrined in the CWEF motto: "A desperate analyst is our best customer."

Lesson Learned: *Go where you are needed and leverage that need to gain operational momentum before you spread yourself too thinly. Wider is not better; at least in the early stages. Reaching critical mass can be slow, but is the only sure way to demonstrate a compelling business case.*

Guideline 6: You need a lot of money to deploy collaboration technologies.

This was not our experience. We wish we had had the benefits of deep pockets, but instead had almost no money to spend. The CWEF is a very small facility, with a correspondingly small budget. It was established as a technology

Balancing the Requirements of Collaboration and Security

By Christine Eliopoulos

In today's high-tech world, just about everyone from the company president to her teenage son has used collaboration tools of one sort or another. The company president sends e-mail memos to her staff, participates in meetings in which participants share presentations online, schedules meetings through the company's electronic calendar tool, and regularly conducts meetings via videoconferencing. Her son spends more time chatting with his friends online than watching television. Chances are, however, neither is very aware of the security shortcomings of many of the collaboration tools they use or the technologies put into place by security administrators or Internet Service Providers (ISP) to protect their computers and networks.

The creators of many commercial collaboration offerings designed them using multimedia and conferencing standards that were not originally developed with security in mind. Although an International Telecommunications Union (ITU) standard for security in multimedia collaboration exists, few if any products are available that claim to implement the standard. Most first-generation applications have been developed with little or no security support, restricting their applicability to environments in which there is a great degree of trust among collaborators and collaboration sessions do not involve sensitive matters. The lack of authentication, access control, and privacy support in these tools requires users to be vigilant in their procedural security and to be particularly conscious of the identities of session participants and their access to local resources.

Balancing the often conflicting goals of collaboration and security is a challenge. To enhance tools to support improved security, vendors must decide where and how much

information-sharing capabilities is encryption-based privacy. Many tools offer privacy support that restricts the exchange of communications to certain named collaborators.



security is needed. Electronic conferencing (e.g., text-based chat, audio, and videoconferencing) and data conferencing applications (e.g., shared whiteboard, application and screen sharing) are likely candidates for improved security features. Authentication and access control are particularly important when using conferencing tools such as application or screen sharing that can afford relatively open access to local desktops or networked resources. Users need a mechanism for identifying collaborators and limiting which files, applications, or portions of a system they may have access to during a collaboration session. The use of audio and video tools can introduce opportunities for compromise as well. When using these tools, remote collaborators have "eyes and ears" into the host's environment that could lead to eavesdropping, at the worst, or embarrassment, at the least. Maintaining a physical presence when these tools are in use can limit potential exposure.

Another feature that would improve the security of most types of conferencing and

Unfamiliar users, however, often confuse this capability with stronger encryption-based privacy. Private chat sessions and point-to-point audio and video are common examples of this weak brand of privacy. While limiting collaborators is sufficient in some environments, other situations require greater assurance and stronger protection from eavesdropping. Use of digital certificates issued from a Public Key Infrastructure (PKI) form the basis for most strong authentication schemes.

Some newer versions of popular collaboration tools incorporate client-server encryption (all exchanges between client and server are encrypted), as well as data encryption for applications such as chat and application sharing. Without built-in application security features users must rely heavily on the elements of trust, perception, and sometimes paranoia.

A major barrier to secure collaboration is found in multicast and H.323-based audio and video tools (see related article on page 3).

“Balancing the often conflicting goals of collaboration and security is a challenge. To enhance tools to support improved security, vendors must decide where and how much security is needed.”

Generally, use of these tools poses problems in environments where collaborators reside on firewalled networks because the tools often require a less restrictive firewall policy than most administrators are willing to permit. Some of the most popular H.323 implementations require the use of dynamic ports for User Datagram Protocol (UDP)-based audio and video streaming and Transmission Control Protocol (TCP)-based call control. Typical packet filtering firewalls don't support dynamic port filtering — they require application-specific proxies or very permissive firewall policies that open a wide range of ports for a potentially large number of hosts. Development of an application proxy is a very difficult task because of the complexity of the H.323 protocol, and opening a gaping hole in your site's firewall is never a good idea. Though some vendors are marketing H.323 firewall solutions, they are not sufficient for many environments. Most experts propose a wait-and-see approach with respect to H.323 through a firewall — that is, wait until a mature application proxy that brokers H.323 communications securely is available before permitting its use through a firewall.

In addition to the H.323 firewall issues, Internet protocol (IP) multicasting — used by many audio and video tools — causes problems when used between firewalled networks. IP multicasting is the transmission of an IP datagram to a set of hosts (i.e., a multicast group) identified by a single IP destination address. Host group membership is dynamic and open; that is, any host may join and leave a group at any time. There is no built-in mechanism for implementing closed groups or communications privacy. Eavesdropping on multicast communications is trivial. Firewalls established as perimeter protection typically block UDP, the transport mechanism for multicast packets. Because of the connectionless nature of UDP, and, in particular, the fact that it does not have flow control or connection direction indication — it is

almost impossible to define a reasonable firewall policy that allows some UDP communications and blocks others. Many of the protocols that are implemented over UDP are easily exploitable. In the case of multicast, security risks are compounded due to the fact that it is used as a mechanism for transmitting a single packet to multiple recipients. As you can imagine, this is a very efficient way of attacking a number of systems simultaneously.

Researchers are working on solutions to address multicast security issues; however, commercial products that implement true multicast security are more than a year or two away. In the meantime, approaches used to tunnel multicast are being used successfully in environments in which the associated security risks are acceptable.

So what does this mean for the company president and her son? In all likelihood the teenager is more worried about his mother listening in on his phone calls than he is about having his conversations with schoolmates snooped or spoofed. The company president has much more at stake. In the absence of security features built-in to the collaboration tools she uses, the president must take special precautions to protect her information from compromise. She should work with her security administrators to ensure that adequate network policies are in place to restrict the use of inherently insecure applications across the company's security boundary. She should make sure that her staff members choose collaboration tools with security requirements and concepts of operation in mind. Most importantly, the president — along with the rest of us — must wait — and anticipate — the contributions that new standards and greater security awareness will make to the collaboration technology market.



For more information, contact Christine Eliopoulos at 781-271-3625 or celiopou@mitre.org

IETF Working Group to Define Presence Information

By Jay Carlson

The Internet Engineering Task Force (IETF) is an international community of stakeholders in the design and operation of the Internet. Participation in the IETF is open to anyone; organizational membership is not required. Work is divided into a number of functional areas, each of which organizes Working Groups on specific topics. One such Working Group is working toward defining protocols and data formats necessary to build an Internet-scale end-user presence awareness, notification, and instant messaging system. Critical issues being address by the group include scalability, privacy, authentication, and user address namespace.

Instant messaging differs from e-mail primarily in that its primary focus is immediate delivery to the end-user. Presence information was readily accessible on Internet-connected systems years ago — when a user had an open session with a well-known multiuser system, friends and colleagues could easily tell from where the user was connected and whether the user was using his or her computer. Since that time, computing infrastructure has become increasingly distributed and a given user may be consistently available but has no standard way to make this information known to his or her peers. Read more about the Internet Engineering Task Force online at http://www.mitre.org/pubs/edge_perspectives/february_00/carlson.html

For more information, contact Jay Carlson at 781-271-2378 or nop@mitre.org



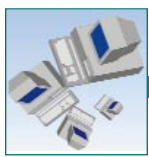
Challenge Problems Guide the Future of Collaboration Research

By Rod Holland

MITRE's collaboration research program, comprised of multiple teams supported by diverse sponsorship, has amassed significant accomplishments in the collaboration arena. MITRE research has elucidated some of the basic technical and organizational principles of the construction and use of collaborative mission environments. This has helped stimulate new operational thinking in our sponsor communities. The various agencies affected are issuing new requirements, and vendors are trying vigorously to deliver commercial products to satisfy them.

In this environment, it is legitimate to pose the question, "What will be the focus of future collaboration research?" Should we declare this area mature and move on to agent technology? Is MITRE's role in collaboration technology now confined to advice on acquisition decisions and similar operational matters?

On the contrary, I believe that much remains for MITRE to do in the field of collaboration research, but only if we continue to break new ground. Breaking new ground in collaboration research requires that we step away from the problems that have become comfortable — work group and small-enterprise-scale collaboration — and focus on a set of new challenge problems. These challenge problems are technically difficult, are important to our sponsors, and are not necessarily going to be solved by the "waiting for COTS" algorithm. Many of the challenge problems are interrelated; multiple investigations across the gamut of difficult topics are required to lay a secure foundation for the next generation of collaboration technology.



Problem 1: Scaling and Distribution

Current systems (e.g., Collaborative Virtual Workspace, GTE's InfoWorkSpace™, Odyssey) have

credibly demonstrated a capacity to serve communities of up to several hundred users simultaneously. The whole Department of Defense (DoD) and the IC (Intelligence Community) can be considered together as an extended community with a head count in the low millions, and an organization count in the thousands or tens of thousands. While individual work groups and organizations may be well served by existing solutions, the liaison and echelon relationships within the larger community are not. Current systems have a centralized client-server architecture, which is unlikely to scale appropriately, and raises issues both of control and of catastrophic failure. Server federation has been proposed as a possible solution for both CVW and InfoWorkSpace, but remains to be demonstrated. More radical approaches, such as fine-grained distribution of collaboration services — a collaboration fabric — may be more promising in terms of scalability and robustness. The COTS experience with very large deployments of instant messaging services needs to be studied.



Problem 2: Heterogeneity

The rapid deployment of the current generation of collaborative environments to the sponsor base has resulted in the creation of what MITRE's Cindy Kabat has termed "islands of collaboration," in which different organizations deploy different systems, thereby compounding the problems already presented by scaling and distribution. If one considers that uniformity by bureaucratic fiat (whether desirable or not) is unlikely to succeed so early in the evolution of a technology, then solving the problems of cross-representation, intercommunication, and document interchange among heterogeneous collaborative environments becomes urgent. More subtle is the problem of collaboration policy automation at organizational boundaries: if my agency is collaborating with your agency, what shall I let you see of my virtual environment, what are

you willing to let me see of yours, and how can we arrange for the automatic enforcement of our respective policies so that we can initiate a collaboration quickly and confidently?



Problem 3: Security

The interaction between collaboration technology, which seeks to make information available to all who need it, and information security, which seeks to ensure that information is provided only to those authorized to have it, is an extremely rich research topic, which should sustain a variety of investigations. For example, anybody trying to provide access to a common collaborative environment across multiple firewalls in a way that satisfies both the operators of the firewalls and the participants in the collaborative environment will appreciate the difficulty of the problem and its immediate relevance.



Problem 4: Tactical/Mobile Collaboration

Existing implementations of collaboration systems, with their centralized server architectures and expectations of relatively benign network environments, are not well suited to the demands of tactical and mobile users. In a tactical environment, servers may come and go — sometimes never to return. Network Quality of Service parameters will typically range from very inhospitable to bizarre. Adequately supporting tactical users requires research in network services, distributed computing, and collaborative Human-Computer Interaction (HCI) domains, and the construction of fieldable prototypes for testing in tactical environments.



Problem 5: The Human Factor

Collaboration technology is ineffective if it is not used.

“No man ever steps in the same river twice, for it’s not the same river and he’s not the same man.”

Heraclitus



Barriers to use may derive from user interfaces, user interaction policies, or user interaction modalities that clash with individuals’ workstyles. Other barriers may derive from a mismatch between group culture and practices and the characteristics of a newly-deployed collaborative system. Investigations in HCI for collaborative environments can address the first problem; organizational behavioral research can shed light on the second. MITRE has made important contributions in these areas and should continue to do so.



Problem 6: Evaluation and Instrumentation

Meaningful, reliable, and reproducible evaluation methodologies for collaborative systems must be developed and employed to stimulate rapid progress in collaboration technology research and to help organizations measure the operational effectiveness of deployed solutions. These evaluation methodologies must be supported by an array of instrumentation techniques for collaborative environments.

MITRE’s strong presence in these research areas provides us with many opportunities to aid our sponsors.



Problem 7: Architectures

The question of how one builds a collaborative environment, or a collaborative mission application, has numerous answers. For example, the question of how one most effectively uses component architectures for both client and server construction is a topic of current investigation. As new technologies

(e.g., Jini™) become available, novel collaboration architectures will suggest themselves and should be investigated. Some may represent real advances over earlier solutions; they may also contain hidden traps for government users. Timely investigation could bring to light problems inherent in new architectures and, perhaps, suggest remedies.



For more information, contact Rod Holland at 781-271-7427 or rholland@mitre.org

OMG’s Open Specifications to Provide Interoperability Solutions

By Jeff Kurtz

The Object Management Group (OMG) is a members-based organization that is creating open specifications to provide interoperability of distributed software and to assist developers in tailoring software to their own needs. The OMG is best known for its object request broker architecture, known as the Common Object Request Broker Architecture (CORBA), a platform and language-independent infrastructure for distributed object interaction. CORBA is just one component in the OMG’s Object Management Architecture (OMA). The OMA also specifies services for object life



cycle management, common facilities for tasks like printing and database access, configurable application-specific objects, and domain-specific interfaces for domains like healthcare or telecommuni-

cations that require interoperability between vendor systems. The OMA is continuously evolving. Several efforts are ongoing in the area of computer supported cooperative work (CSCW). Read more about the Object Management Group and CSCW Technology online at http://www.mitre.org/pubs/edge_perspectives/february_00/kurtz.html



For more information, contact Jeff Kurtz at 781-271-2291 or jkurtz@mitre.org

“[It] is precisely because IT elements do not themselves perform core mission functions [that] they can often miss the potential value that such disruptive technologies provide.”

Collaboration Technology Insertion
continued from page 5

discovery and risk mitigation facility on the premise that if it failed, the damage would be small. If it succeeded, however, the potential payoff would be (and has been) immense.

When we began this effort, we had no server, no virtual network, no client distribution facility, no headsets, microphones, video cards, or any other hardware supportive of desktop collaboration systems. We had to “liberate” the equipment.

After our first pilot activity proved the concept while running on a small work group server, we noticed that one of the SUN Enterprise Servers at the agency was not yet assigned an operational support role. We made an unsolicited proposal to use this server as our home collaboration server, and in negotiations agreed to split its use with another service for a year. That was two years ago and we now control this server and apply it exclusively to CWEF initiatives.

Having a large server with considerable excess capacity has enabled us to provide collaborative services to a growing audience without concern over computing resources.

We needed hundreds of software router hosts for our virtual MBONE and we had no money with which to purchase them, so we liberated them. We found a cache of several hundred surplus Sparc IPX machines in the excess equipment warehouse. Because they had no remaining utility as user desktops, they were waiting to be decommissioned, but were perfectly suited as multicast routers.

Lesson Learned: Sometimes you have to appropriate the needed resources in nontraditional ways

Summary

Conventional technology transfer wisdom is written to address evolutionary technologies,

which provide improvements to current business practices. These technologies do not generally pose threats to the culture or structure of large organizations. *Disruptive technologies*, on the other hand, offer previously unforeseen means of reforming an organization’s business model, with concomitant changes to structure and culture.

Collaborative systems are disruptive by their very nature, because their application forces a redefinition of existing business practices and the associated organizational structures and cultures that support them. This often means that those elements most committed to sustaining the current business model can be effective obstacles to the introduction of collaboration frameworks. In large organizations, it is the IT support elements that sometimes are most committed to the status quo, and surprisingly not the line organizations they support. Perhaps this is because IT elements do not themselves perform core mission functions and they can often miss the potential value that such disruptive technologies can provide.

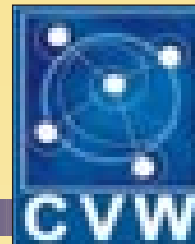
By starting small with a core of dedicated analytic leaders who do perform those core functions, we were able to achieve mission success without making a large financial investment. Building on that success, we were able to innovate, adapt, and appropriate resources, while clawing our way into the mainstream IT enterprise structure. Had we tried to get there any other way, the structure itself would have effectively blocked our progress.

These lessons will be useful to other technology insertion efforts underway in similar settings within the Government, and that through their application, the national good can be served.



For more information, contact John Davidson at 410-850-4892 or davidson@mitre.org

CVW Evolves as Open Source



By Rob Leslie

Following years of successful research and piloting of collaboration services, on March 31, 1999, The MITRE Corporation made its Collaborative Virtual Workspace™ (CVW) software publicly available as Open Source on <http://cvw.mitre.org/>.

CVW’s release as Open Source stimulates collaboration research and fosters the creation of commercial place-based, persistent, computer-mediated collaboration products. The competitive market that the Open Source project is intended to create serves MITRE’s sponsors by creating commercially available, affordable and supportable products based on MITRE’s research and piloting.

MITRE will moderate software integration, review code contributions and publish new versions of the core code base, maintain a Web site to support CVW as a research project, and stimulate technology transfer and collaboration research. Already, approximately 9,000 copies of the CVW source code have been downloaded from the Web site. Of the software recipients who identified themselves, 17 percent were from commercial entities.

Several companies are leveraging CVW for their commercial products in different ways, such as providing training for CVW, deploying and supporting CVW, using CVW as an environment for continuing research of collaborative systems, and using CVW as a proof of concept.

As a user and integrator of multiple collaboration environments, MITRE is working closely with its sponsors and commercial corporations to create standards, bridges, and gateways — in general, interoperability — among collaboration tools.



For more information, contact Rob Leslie at 781-271-2962 or rob@mitre.org