

NEWS RELEASE

For immediate release: Feb. 6, 2009

Contact: Mr. Jamie Abel, Media Relations Manager, Ohio Supercomputer Center/OARnet, 614-292-6495, jabel@osc.edu

Secure videoconferencing provides key to enhancing education, research collaboration, savings

OARnet study seeks balance of security, quality in videoconferencing

Columbus, Ohio — Some technologists see a day in the not-so-distant future when advances in videoconferencing will allow the quickly maturing technology to greatly enhance distance education, boost research collaboration and reduce travel and meeting costs.

“Network-based video in its many forms, including IPTV [TV over the Internet], surveillance, teleconferencing and mobile, is rapidly becoming a key service within every community – academia, consumer markets, enterprise, government and K-12 education,” said Loki M. Jorgenson, Ph.D., chief scientist with Apparent Networks Inc., a research partner of the Ohio Academic Resources Network (OARnet).

Network engineers at OARnet recently addressed one of the remaining technological hindrances to widespread use – balancing network security with superior performance. The team collaborated with specialists from the Ohio Supercomputer Center (OSC), The Ohio State University, Edgewater Networks and Polycom on a yearlong study, “Secure Videoconferencing: Balancing Multimedia Performance and Data Security Tradeoffs,” funded by the Ohio Board of Regents and Polycom.

“A high-quality, easy-to-configure videoconference capability throughout the University System of Ohio is essential to dramatically improve and expand distance education,” said Ohio Board of Regents Chancellor Eric D. Fingerhut. “Secure, high-quality videoconferencing can provide more Ohioans with the opportunity to gain a college education without extensive back-and-forth travel to a campus. It also can increase academic offerings from distant institutions available to students, enhance collaboration in research and administration, and reduce campus travel expenses for campus faculty and staff.”

“Network planners continually face challenges that involve balancing trade-offs between network security for data and performance of voice and video,” said Prasad Calyam, Ph.D., a senior system developer/engineer at OSC and OARnet. “The primary challenge is in configuring firewalls to allow voice and video traffic in and out of the internal-network’s ports, while limiting malicious access of internal-network data by intruders through the same open ports. Improper policy decisions and policy mis-configurations in firewalls could result in vulnerable networks, slow data transfers as well as create voice and video performance problems.”

The engineers extensively analyzed new videoconferencing standards and vendor solutions from organizations such as Polycom, Cisco and the GNU Project, identifying the limitations and caveats that exist in their adoption. Based on the experiences from these studies, OARnet engineers developed a list of “best practices” for deploying small-to-large scale secure videoconferencing deployments in campus and enterprise networks.

-more-

OARnet was established by the Ohio Board of Regents in 1987 to provide researchers with access to the computational resources of the Ohio Supercomputer Center. Today, OARnet provides Ohio’s colleges and universities and their research partners with an integrated technology infrastructure that includes unrivaled intrastate network connectivity and shared services. OARnet specializes in providing custom solutions, whether providing virtualization resources, spanning the globe by videoconference or providing unrivaled 24/7 network support. For more information, visit www.oar.net.

The list of best practices addresses resource planning, adequate bandwidth, conflicting solutions, fail-over options, dedicated servers, and testing and documentation.

“Polycom was impressed with the experiments ... performed in comparing various firewall traversal solutions,” said Kurt Peterson, regional director for Polycom. “The experiment results clearly identify the deployment limitations and tradeoffs involved in balancing security of data and performance of video. The best-practices for secure videoconferencing proposed also provide sound advice to network engineers.”

-30-

Editor's Note: *An electronic copy of the full report can be obtained at:*
<http://www.osc.edu/press/releases/2009/secure.shtml> .