

United States Department of Energy
Office of Energy Research
Office of Basic Energy Sciences
Energy Research Financial Assistance Program

Notice 98-02

Building EPSCoR State/National Laboratory Partnerships

**EVALUATING AND OPTIMIZING NETWORK SECURITY AND
PERFORMANCE IN SCIENTIFIC DATA DISTRIBUTION SYSTEMS**

submitted by

University of Wyoming

in partnership with

Pacific Northwest National Laboratory, DOE

Principal Investigator:

Rex E. Gantenbein, Ph.D.

Professor

Department of Computer Science

University of Wyoming

Laramie WY 82071-3682

Phone: (307) 766-4226

FAX: (307) 766-4036

E-mail: rex@uwyo.edu

EVALUATING AND OPTIMIZING NETWORK SECURITY AND PERFORMANCE IN SCIENTIFIC DATA DISTRIBUTION SYSTEMS

Abstract

The increasing use of computers to control scientific experiments, coupled with the phenomenal growth of computer internetworking as a communications medium, has greatly expanded the ability of scientists and engineers to collaborate on research over great distances. Experimental data can be acquired and shared among geographically separated computers; experimenters can use telecommunications to remotely access and control laboratory apparatus. Using public networks, such as the Internet or the forthcoming Internet 2, is attractive for such collaboratory systems due to their accessibility, ease of use, and relatively low cost. However, the dual problems of performance and security in using a public network must be addressed, in order for this technology to reach its full potential.

Many mechanisms exist for supporting secure remote access to scientific experiments over public computer networks, but there has been little study of the effect of these mechanisms on the performance of the data distribution system and the fidelity of the data shared among the collaborators. This project involves the development of models and tools for evaluating the effects of integrating security and data distribution into a scientific data collection system. We will develop software for monitoring and analyzing performance, security, and data quality in a scientific data distribution system and will show how the models embodied in the software can be used to optimize existing collaboratory systems with respect to these properties. The end result will be a suite of tools and techniques for evaluating security and performance in systems using public networks for collecting and distributing scientific data over a distance.

EVALUATING AND OPTIMIZING NETWORK SECURITY AND PERFORMANCE IN SCIENTIFIC DATA DISTRIBUTION SYSTEMS

Project Description

Objectives

The overall goal of the proposed research is the development of techniques and tools for the modeling and evaluation of mechanisms by which energy-related scientific data, collected by computer-controlled experimental instruments, can be securely and efficiently gathered and distributed to geographically dispersed scientists and engineers. Mechanisms exist for using computer networking to achieve secure remote access to

scientific apparatus, but there has been little study of the effect of these mechanisms on the performance and transmission quality of the network. It is essential to understand the interaction of performance, security, and transmission quality in order to optimize scientific data distribution systems with respect to these factors.

The specific objectives of this project are: (1) to create models and software for analyzing performance, security, and data quality in networked scientific data distribution systems, and (2) to improve techniques for remote data collection and distribution, based on results from applying these models to existing systems. The result of this work will be a suite of techniques and software support tools for evaluating such systems and optimizing them for secure, efficient remote experimentation.

This project will establish a partnership between the University of Wyoming (UW) and Pacific Northwest National Laboratory (PNNL). PNNL personnel will provide knowledge and examples of systems for secure remote collection and distribution of scientific data. UW researchers will provide expertise in the development of modeling and evaluation tools for analyzing security, performance, and quality in networked systems. UW students and faculty involved in the research will have opportunities to participate directly in projects at PNNL, while PNNL researchers will be provided with reports, demonstrations, and software for analyzing their systems. The partnership established will take advantage of a unique combination of capabilities to further the research missions of both organizations.

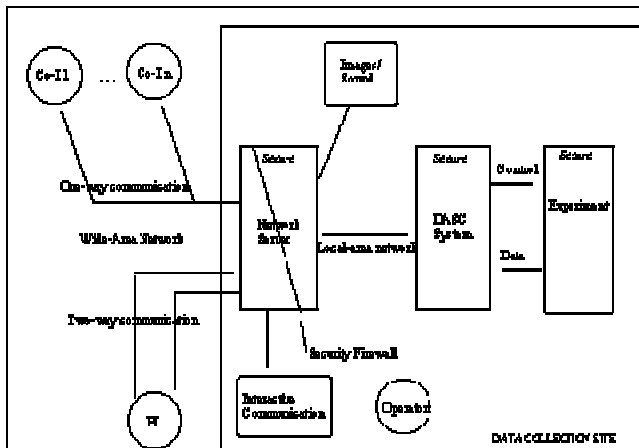
Data Distribution Systems and Scientific Collaboration

Scientific collaboration has historically relied on frequent interaction among scientists, engineers, administrators, etc. Researchers in many disciplines have reaped significant benefits from sharing results and discussing their work with others. While scientific meetings and archival publications have long served as a medium for communicating results to interested colleagues, more frequent and less formal exchanges of ideas are also beneficial to the process that creates those results. Until recently, such exchanges could only be accomplished through face-to-face meetings at a central site or laboratory, through the mail, or by telephone, but the pace of modern research requires more timely and less costly means of distributing information. Furthermore, the scope of many problems, especially environmental and energy concerns, reaches beyond the boundaries of a single lab, agency, or even nation, and solutions require a cooperative effort that can span not only time zones, but continents and cultures.

The advent of computers and the recent growth of tools for telecommunications networks have greatly expanded researchers' abilities to communicate more quickly, easily, and completely over long distances. In particular, several tools exist that support *collaboratories* [1], integrated networks of computer systems that create virtual environments for remotely collecting and sharing experimental data. This new paradigm for scientific collaboration has the potential to both accelerate the development and dissemination of basic knowledge and reduce the time between the discovery of a result and its application in the real world [2].

Among the existing tools that can contribute to a collaboratory are shared electronic notebooks that are read and updated by all investigators in a project, electronic mail and mailing lists for fast communication among participants and interested observers, World-Wide Web (WWW) links to sources of background information, and Internet journals for timely publication of results [3]. Perhaps the greatest potential value of a collaboratory system, however, is the ability to use computer networking to access experimental apparatus and collect data from experiments from afar. Today, computers are widely used to control complex scientific instruments and collect the data from experiments for analysis. With telecommunications technology, computers at geographically distant sites can be connected to these control computers, supporting a wide range of techniques for remote access to scientific instruments as well as for distributing data collected from instruments to collaborators at various sites around a lab, a country, or the world.

We can refer to systems like this as *scientific data distribution* (SDD) systems, since they distribute scientific data over long distances. SDD systems support collaboratories both by sharing data and by providing remote access to experiments, using networks of computers (local-area networks, which cover small geographic areas such as a single building or laboratory, or wide-area *internetworks* that connect local networks together over large geographic areas) to link individual workstations performing computational tasks into a cooperative, coordinated system.



SDD systems are typically constructed using a *distributed computing* architecture, like that shown in Figure 1. In this architecture, a network server connects a computer-controlled scientific instrument with computers at remote sites such as laboratories or offices. In essence, telecommunications links eliminate the need for the physical presence of observers at the experiment site by carrying data, images, and sound from the site to the observers. A *primary*

observer controls the experiment through a two-way connection with the experiment control computer. Additional *secondary* observers with one-way connections to the site view the experiment in either real time (that is, as the experiment is being performed) or in store-and-forward mode (the activities and results of the experiment are recorded on the control computer and then played back by viewer software on the observer's computer).

Performance and Security in Scientific Data Distribution Systems

Two obvious problems must be solved, however, for collaboratories in general, and SDD systems in particular, to fulfill their promise. The first of these is performance. While the speed of transmission of information across telecommunications networks far exceeds the

dreams of even twenty years ago, many applications (scientific and otherwise) require consistently high transmission rates to satisfy the expectations of their users. Dedicated networks based on satellite technology, private "closed-path" links, or ISDN technology can provide these kinds of rates, but they are expensive to create and difficult to maintain. Public internetworks are less expensive, widely accessible, and easy to use. However, this accessibility, coupled with the relatively low cost, has increased the traffic on these networks to the point that consistent access and transmission rates cannot be achieved.

The second problem is security. Networks of computers, particularly public networks like the Internet, are notoriously susceptible to security failures. Typically, these failures fall into one of two categories: unauthorized access to computers connected to the network, and breaches of confidentiality for data stored on or transmitted between those computers [4]. Both are causes for concern when network access to scientific experiments is possible, particularly where the information being collected is of a sensitive or classified nature.

The confidentiality of data in a networked system can only be assured if a strong defense exists against unauthorized access to the system [5]. Security mechanisms are available for public networks, ranging from encryption on transmitted data to user authentication and authorization schemes to prevent unwanted access [6,7]. However, it is not yet well known what level of security can be achieved for systems using public networks, or how security mechanisms affect the performance of such systems. The objective of this project, therefore, is to develop models and tools for evaluating data distribution and protection mechanisms and use the results of these evaluations to improve the performance and security of SDD systems.

Related Research

PNNL: Network tools for scientific collaboration

PNNL's core mission is the delivery of environmental science and technology in the service of the nation and humanity. Central to this mission is the William R. Wiley Environmental Molecular Sciences Laboratory (EMSL), a new national scientific user facility that provides advanced experimental and computational capabilities for solving environmental problems to the worldwide scientific community. Among the ways in which these facilities are provided is through the EMSL On-Line (EOL) project, which supplies EMSL scientists and their collaborators with on-line Internet access to the laboratory's experimental apparatus, data, and research results as part of the DOE's Distributed Collaboratory Experiment Environments Program [2]. This project integrates EMSL's Collaboratory -- a WWW-based system that allows real-time remote collaboration, interaction with remote instruments and software, and access to remote data and visualizations -- with videoconferencing tools, electronic notebooks, and shared computer displays in the nuclear magnetic resonance (NMR) spectroscopy domain.

Through the EOL facilities, an inter-laboratory group of DOE researchers has been able to remotely and securely control and monitor the NMR spectrometers at EMSL, access

data, analyze and visualize results, discuss findings, and prepare proposals, presentations, and papers. Researchers conducted a series of experiments on a heat shock factor protein that was prepared at one laboratory and shipped to EMSL for analysis on a high-resolution spectrometer. Participants in this experiment acquired data on the protein through remote control of the spectrometer, then used videoconferencing, electronic notebooks, and shared real-time computer displays to share results and prepare documents.

Work has also been done at EMSL to integrate a "secure shell" application (developed by another group at PNNL) into this environment to allow secure remote login to the NMR spectrometer console and encrypted transmission of the console display back to the remote user. In addition, a secure shared view of the console to multiple sites was demonstrated by integrating this secure shell with the EMSL videoconferencing system.

UW: Evaluating and improving security, performance, and reliability in distributed systems

The Department of Computer Science at the University of Wyoming has applied much of its research effort for the past twelve years to distributed computing systems. Of particular relevance to this project is the work done by the PI and his research group in evaluating and improving the security, performance, and reliability of such systems, especially systems for the geographic distribution of data. We have created a prototype system called TELELAB that supports remote access to scientific data acquisition over the Internet using TCP/IP protocols to connect client software with the control system [8]. This system uses an object-oriented architecture to allow its customization for a variety of applications, although its primary target is the collection of biomedical data for human health research [9].

Related work in security has primarily centered on detecting unauthorized attempts to gain access or corrupt data on systems [10]. We have shown that a *resource broker* approach [11], shown in Figure 2, can be used to achieve security efficiently in a distributed architecture. A broker is an agent process created when an application is initiated to manage resources needed by that application. Resource requests from the application's clients are sent to the broker for processing. As clients are admitted to the application, they have access to all the resources known to the broker. The broker must authenticate a client attempting to join an application before the client becomes a member of that application.

Since the brokers -- not the clients -- determine who has legitimate access to resources, the brokers form a *security firewall*, as shown in Figure 1 above, that can prevent unauthorized access to any resource in the system. We are currently applying the broker approach to the TELELAB system to evaluate its ability to support secure data distribution over the Internet [12].

Other research at UW related to this project involves the modeling and evaluation of distributed systems. We have carried out several projects, largely sponsored by NASA, to

study both existing and proposed computer systems and evaluate various properties, including their dependability and performance [13-16]. In this work, we have created formal models for determining the properties of the systems based on measurable characteristics of the system, then created software tools for monitoring and evaluating the systems' actual behavior with respect to these properties. This work has proved valuable both in finding design flaws that could affect the dependability of a system and in improving the performance and quality of the system implementation.

Research Plan

The specific aim of this research is to create models and software tools with which we can evaluate and optimize the ability of telecommunications networks to support secure and efficient scientific data distribution. The basic questions to be answered by this study include the following:

- (1) What existing (or developing) telecommunications technologies can be used to provide remote access to computer-controlled scientific experiments from geographically separated researchers?*
- (2) How can remote control of an experiment and the distribution of collected data be provided without compromising the security, integrity, or availability of the experiment?*
- (3) When access to scientific experiments is made available over a telecommunication network to authorized users, what effects does this have on the experiment itself?*
- (4) What benefits are accrued from networked collection and distribution of scientific data and what are the costs and trade-offs associated with these activities?*
- (5) What are the limitations of the technology for scientific data distribution, and what additional support is needed to transfer the technology to the public sector?*

To answer these questions, UW researchers, in cooperation with PNNL scientists and engineers, will develop models and mechanisms for evaluating the performance, quality of transmission, and level of security of SDD systems. A computer-controlled experiment testbed, to be constructed at UW, will provide an environment similar to those in use at PNNL for validating the models and testing software tools for monitoring and analyzing SDD systems with respect to performance, security, and data quality.

Modeling refers here to developing tools and techniques to assess the behavior of a computer system. This activity is important in evaluating the system with respect to particular properties (such as performance, security, and quality of information transmission). By isolating factors that affect such properties, models can be created that allow these factors to be varied and the effects of the variances analyzed. Models may be either *predictive* (that is, intended to predict the behavior of a system independent of its implementation) or *descriptive* (that is, used to monitor the behavior of an existing system) with respect to the factors being analyzed. While predictive models are useful in

guiding the design of a system, descriptive models apply to existing systems (or prototypes of such systems). These models are usually more accurate than predictive models and allow more direct recommendations for optimizing the modeled properties to be made.

Performance models

We will develop descriptive models for measuring performance and overhead for the remote access and control of experiments and the distribution of data from a remote site to the observer(s). Factors to be used to evaluate performance will include:

- throughput of information for the various components of an SDD system, both with and without security features installed;
- response times of the requests for access or data from the remote sites;
- locality of memory references in the local-area network;
- communication bandwidth achieved in both the local- and wide-area networks;
- processor speed available in each of the nodes of the system; and
- transmission latency over the wide-area network.

Information about these factors will be gathered through the use of monitoring software, which we will develop based on our models. The monitoring software will be designed to avoid biasing the performance results as little as possible. The performance data gathered in this way can then be used to compute estimates of the peak and nominal efficiency, availability, and reliability of an SDD system. We will create an integrated software tool to compute the following standard measures for these properties [17], based on data gathered from the monitoring software:

- efficiency: the ratio of the usable system capacity to the nominal capacity under ideal workload conditions;
- availability: the percentage of total time during which the system is available for use; and
- reliability: estimated mean time interval between two consecutive failures.

Estimates of these factors will help evaluate the effectiveness of various mechanisms for securely distributing data and allow comparison among alternative implementations of the mechanisms. We will use object-oriented design principles to assure that the monitoring and analysis software we develop will support evaluation for a variety of SDD systems with minimal revision.

Quality of transmission models

Clearly, the acceptance of any SDD system by its users depends on the quality of the transmission link between the sending and receiving sites. This "quality" is difficult to measure in a quantitative way. Performance measures such as those described above can provide some indication of the quality of the transmission, but many other measures are subjective: fidelity of data or commands transmitted from one site to another, visual impressions of transmitted images, location of information on the workstation screen, even ease of use of the interfaces for remote experiment control.

We believe that a descriptive model for local-area network fidelity of data, based on the architecture for SDD systems shown in Figure 1, can be constructed by comparing original data generated by an experiment against the version of the data received by the network server. We can therefore evaluate fidelity of locally transmitted data using a simple side-by-side comparison program. Where security concerns require data to be encrypted, the transmitted data fidelity can be evaluated by comparing it to encryptions of the original data.

In addition to using side-by-side comparisons to measure fidelity in wide-area data transmission, we propose to develop additional models for the more subjective qualities of data distribution that can be evaluated through the use of automated checklists. The desirable properties for such transmission will be elucidated by interviews and questionnaires with end users of the data distribution system and composed into a checklist. The checklist will then be implemented in software and integrated into the system so that users can complete it during tests of the system; the responses will be automatically tallied and analyzed. Features perceived by these users as less than adequate can then be reviewed and improved where possible. Repeated tests and statistical analysis will ensure the validity of the responses as well as isolate any transient events.

Security models

Security is often viewed as a binary property: either a system is secure or it is not. In reality, however, most systems can be viewed as supporting *levels* of security ordered by the accessibility of the objects at each level. (As an example, the military classifications of unclassified, classified, secret, and top secret represent increasing levels of security.) Once the classes in an information system are established, the flow of information among the classes can be controlled by protocols to ensure no information is ever transferred to a lower security level.

We propose a model for security for SDD systems based on three distinct levels: *secure* information that is protected from all external access; *confidential* information that is accessible only with proper authentication; and *open* information that is generally accessible (within the usual protection guidelines for network access). Users can be assigned authorizations that specify their ability to access each of these levels, and

mechanisms developed that protect information stored or transmitted in such a system at each level.

Using this model, we will evaluate multiple protocols for collection, transmission, and viewing of distributed data with respect to security using scenario analysis [18]. Scenarios will be created as both intentional and unintentional attempts to exceed an authorized level of security by a user and observe the results. These scenarios, which we will construct using a scripting language that will allow them to be applied and the responses collected automatically, will individually test each level of security for every object in the system and determine where the weak points lie in the security mechanisms.

Evaluation testbed

As we create models for evaluating performance, transmission quality, and security in SDD systems, we must assure ourselves that the models reflect the reality embodied in the systems. One way to do this is to construct a testbed for evaluating the systems according to the models. This approach has been successfully used in previous studies at UW for evaluating performance and reliability in other distributed systems.

In this project, we will base the testbed on TELELAB, a "virtual laboratory" providing remote acquisition and distribution of scientific data, developed in the UW Distributed Computing Laboratory (DCL) and written in LabVIEW, a language widely used for developing data acquisition systems [19]. The system contains three components, shown in Figures 3A, 3B, and 3C:

- 1) A *data acquisition* program, which collects real-world data, converts it to digital form, and saves it on the data acquisition computer using analog-to-digital conversion boards.
- 2) A *proxy server* program, which uses TCP/IP networking protocols [20] to support interaction between the data acquisition and remote computers, making data from the data acquisition program available for network access.
- 3) A *client* program, which can be run on any computer that supports LabVIEW and has an Internet connection. This program interacts with the proxy server to access data and display it in a continuous stream, similar to the display on the acquisition computer itself. It can also send commands that will remotely start, stop, and configure an experiment.

The mechanisms used in TELELAB closely resemble those used in PNNL's EMSL On-Line project, so (once we have assured its correspondence with PNNL's systems) we can use TELELAB's remote experimental access and control mechanisms to validate the models for performance, transmission quality, and security and to test the monitoring software tools. The analysis of these parameters will help us calibrate the models for more accurate evaluation as well as optimize the testbed's mechanisms for peak effectiveness.

Once these models and tools have been validated in the context of the TELELAB testbed, we can adapt and apply them to existing and developing systems at PNNL to further study the interaction among networking and security factors in SDD systems and look for ways to optimize the effectiveness of these systems. Follow-up research will involve working with PNNL's systems and using the models and tools from this study to evaluate and optimize them.

Project Schedule

The three-year duration of the project will consist of three phases, one for each year.

Phase 1 (September 1998 - August 1999). This phase will begin with evaluating the scientific data distribution systems at PNNL to assure that our testbed accurately reflects them with respect to remote access and control mechanisms, and that the mechanisms to be evaluated reflect the most up-to-date technologies available. At the same time, we will begin setting up the testbed, including acquiring new equipment, porting the existing system to the new platform, and training the research assistants. We expect to have this activity completed by January 1999.

The next step will be to create the performance models for the testbed. This work should be completed within six months. During the remainder of the period, we will create the software for monitoring and analyzing the performance of the system and develop a test plan for collecting the needed parameters. The results of this work will be documented by (1) a report outlining the performance evaluation measures to be used and (2) demonstrations of the performance monitoring and analyzing tools for PNNL personnel.

Phase 2 (September 1999 - August 2000). The initial activity in this phase will be to study the security protocols in PNNL's existing SDD systems and compare them to the security protocols in the testbed. Once the designs of the protocols are compared and the testbed refined to assure its accurate representation of security as used by PNNL, we will use the monitoring and analysis software created in Phase 1 to evaluate the performance of the system with the security protocols in place. This will involve creating the security scripts and the support structure for applying them to the testbed and collecting the results.

We will concurrently develop the quality models, both for transmission fidelity and other subjective factors, in the latter case working with PNNL researchers on the properties needed for the checklists and developing a plan for collecting the results of the tests. Again, on completion of this phase, we will report on our models and tools for evaluating security and demonstrate their capabilities on the testbed for PNNL researchers.

Phase 3 (September 2000 - August 2001). In this phase, we will initially create the software for evaluating transmission quality and fidelity, including the side-by-side comparison program and the automated checklist tool. We will then use these tools to evaluate the quality of network transmissions in the testbed for both local- and wide-area connections, which we will achieve by installing client software on remote computers in

the DCL and at PNNL. We will present to PNNL researchers a full-scale demonstration of the monitoring and analysis tools, and we will summarize our findings in a final report outlining recommendations for applying these tools and techniques to PNNL's SDD systems.

Personnel

The PI for this project will lead the research team, developing the models for performance, security, and quality evaluation, coordinating efforts with PNNL researchers, and supervising the research assistants. One assistant, a graduate student in computer science at UW, will be responsible for maintaining the testbed and developing the software for performance monitoring, security scenario testing, and the automated checklists. The second assistant, an undergraduate in computer science at UW, will be responsible for programming the software for performance analysis and data fidelity comparison, as well as distributing and collecting the questionnaires and interview materials for the checklists. (The graduate student involved in this project will be a Ph.D. candidate, and the work from this project will make up his/her thesis work. It is possible that more than one undergraduate student will be involved over the three-year duration of the project.) Both students will assist the PI in preparing reports and research papers on the results from this work.

During the academic year, student work will be carried out at UW. Each summer, both students, as well as the PI, will have residencies at PNNL to work more closely with the researchers there on adapting UW research to PNNL's needs, as well as learning more about PNNL's activities and systems.

Relevance to Laboratory and University Programs

We expect this research to produce tools by which we can achieve a better understanding of the benefits and costs associated with scientific collaboration over computer networks, particularly the effects of remote access and security protocols on each other and on the quality and fidelity of scientific data gathered from remotely controlled experimental instruments. While certain costs for scientific research can be reduced through use of data distribution systems, and benefits such as convenience and concurrent data analysis accrue, other costs will increase. Our studies will provide the tools and techniques to determine what "price(s)" must be paid to achieve a given level of performance, security, and data quality.

Remote access and data distribution technology can be applied to many energy-related applications, such as environmental testing or Superfund site monitoring. The results of this study should prove especially valuable to environmental researchers interested in sensing and measurement of environmental contaminants, particularly in remote or hazardous locations, where the benefits of automated diagnostic and control systems are particularly important. These areas are specifically included in PNNL's core competencies as identified in the institutional plan [21].

In addition, the development of higher performance and more secure data distribution systems has significant potential in the area of telemedicine, the use of telecommunications and collaboratory systems to improve human health-care delivery. While telemedicine technology development has up to now concentrated on videoconferencing and electronic delivery of static patient information (X-rays, medical records, etc.), scientific data distribution can add a new dimension to health care in remote areas by supporting real-time monitoring of vital signs and health data from a distance. One of the major initiatives at PNNL is applying existing capabilities and technologies developed for other mission areas to the issue of national health care, in particular finding innovative ways to improve health-care delivery systems [22]. The results of the proposed research should be applicable to such systems, particularly in the area of maintaining the confidentiality of patient records distributed over public networks.

Biographical Sketch of Principal Investigator

Rex E. Gantenbein is a Professor of Computer Science at the University of Wyoming, where he teaches classes in software engineering and does research on telemedicine and security in networked computer systems. He has been with the University of Wyoming since 1985. He is also an Adjunct Professor in the College of Health Sciences at the University of Wyoming and an affiliated faculty member of the Department of Medical Education at the University of Washington in Seattle. His previous professional experience includes work as an industrial engineer for Sundstrand Corporation and mathematics assessment test editor for the American College Testing Program.

Dr. Gantenbein is the author of several research papers that have appeared in journals such as the *Journal of Systems and Software*, *International Journal of Reliability, Quality, and Safety Engineering*, *CrossTalk: The Journal of Defense Software Engineering*, and *International Journal of Computer Science and Information Systems*. In addition, he has presented numerous papers at international scientific conferences. These papers and presentations have covered areas such as validating safety-critical system designs through prototyping, adaptive fault management in survivable distributed systems, recovering from a computer virus attack, Internet-based systems for distributed data acquisition, systemic-functional linguistics in writing tools for research papers, and using modeling to design highly reliable software systems. He has received support for his research from NASA, the National Science Foundation, the Wyoming Space Grant Consortium, Intel Corporation, Motorola, and the U.S. Air Force Office of Scientific Research.

He received a B.S. degree with Honors and Distinction in mathematics from Iowa State University in 1972. He received his M.S. and Ph.D. in computer science from the University of Iowa in 1983 and 1986, respectively, under the direction of Dr. Douglas W. Jones. The title of his Ph.D. thesis was "Dynamic Binding of Separately Compiled Objects Under Program Control."

He is currently President of the International Society for Computers and Their Applications and a member of the ACM and the IEEE. He was elected to membership in Sigma Xi, The Scientific Research Society, in 1995, and is included in several Who's Who publications. He was a visiting scientist in the Space Biomedical Research Institute of NASA Johnson Space Center from 1994-1995, and received faculty research fellowships from NASA and the U.S. Air Force.

In addition to his technical interests, Dr. Gantenbein's interests include the ethics of computer use, particularly computer reliability, security, and privacy issues. He is an affiliate of the Wyoming Center for the Advancement of Ethics, and has given several public talks on issues of free speech and privacy as a member of the Wyoming Council for the Humanities Speakers Bureau.

Bibliography

- [1] V.C. Cerf et al, *National Collaboratories: Applying Information Technologies for Scientific Research*, National Academy Press (1993).
- [2] R.T. Kouzes, J.D. Myers, and W.A. Wulf, "Collaboratories: Doing Science on the Internet," *Computer* 29,8 (August 1996), 40-46.
- [3] H. Brody, "Wired Science," *Technology Review* 99,7 (October 1996), 42-51.
- [4] H.J. Smith, "Privacy Policies and Practices: Inside the Organizational Maze," *Comm. ACM* 36,12 (December 1993), 104-122.
- [5] J.I. Schiller, "Secure Distributed Computing," *Scientific American* (November 1994), 72-76.
- [6] R. Oppliger, "Internet Security: Firewalls and Beyond," *Comm. ACM* 40,5 (May 1997), 92-102.
- [7] R.J. Anderson, "Why Cryptosystems Fail," *Comm. ACM* 37,11 (November 1994), 32-40.
- [8] R.E. Gantenbein, Thomas L. James, John R. Cowles, and William H. Paloski, "TELELAB: A Virtual Laboratory for Acquisition and Distribution of Scientific Data on the Internet," 13th Int. Conf. on Computers and Their Applications (to appear March 1998). Available at <http://www.cs.uwyo.edu/~rex/telelab2.html>.
- [9] R.E. Gantenbein and W.H. Paloski, "Object-Oriented Software for Real-Time Biomedical Data Acquisition and Stimulus Control," *Proc. ISCA Int. Conf. Computer Applications in Engineering and Medicine* (March 1995), 21-25.
- [10] F.G.F. Davis and R.E. Gantenbein, "Recovering from a Computer Virus Attack," *Journal of Systems and Software* 7,4 (December 1987), 253-258.

- [11] R.E. Gantenbein, "A Object-Oriented Model for Secure, Biomedical Data Acquisition and Stimulus Control Systems," *Proc. 11th Int. Conf. On Computers and Their Applications* (March 1996), 170-173.
- [12] R.E. Gantenbein, "Secure Remote Access to Physiological Data," (abstract), *Proc. 12th Man in Space Symposium* (June 1997), 150-151.
- [13] R.E. Gantenbein and S.Y. Shin, "A Practical Method for Design Verification of Critical Software Systems," *CrossTalk: The Journal of Defense Software Engineering* 8,8 (August 1995), 23-26.
- [14] R. Gantenbein, S. Roach, and M. Zimmerman, "Software Prototyping as a Tool for Evaluating Real-Time Fault Management Algorithms: A Case Study," *Int. Journal of Computer Science and Information Systems* (to appear).
- [15] R.E. Gantenbein, J.-K. Hong, and S.Y. Shin, "Validating Embedded System Designs Through Simulation," *Int. Journal of Computers and Their Applications* (to appear September 1998).
- [16] S. Shin, C. Shim, and R.E. Gantenbein, "The Optimal Data Interval for Message Passing to Update Checkpointed States in Fault-Tolerant Distributed Systems," 13th Int. Conf. on Computers and Their Applications (to appear March 1998).
- [17] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Testing*, John Wiley and Sons (1992).
- [18] P. Hsia et al., "Formal Approach to Scenario Analysis," *IEEE Software* 11,2 (March 1994), 33-41.
- [19] G.W. Johnson, *LabVIEW Graphical Programming: Practical Applications in Instrumentation and Control*, McGraw-Hill (1994).
- [20] D. Comer, *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Prentice-Hall (1988).
- [21] Pacific Northwest National Laboratory, "Laboratory Mission and Core Competencies," WWW Document <http://www.pnl.gov/glance/instplan/2.html>.
- [22] Pacific Northwest National Laboratory, "Laboratory Initiatives," WWW Document <http://www.pnl.gov/glance/instplan/4.html>.