

Implementing a Scalable Test Environment Simulation for Cyber Warfare

John J. Tran, Ke-Thia Yao & Robert F. Lucas

**Information Sciences Institute/USC
4676 Admiralty Way, Suite 1001
Marina del Rey, California
{jtran, kyao, & rflucas} @isi.edu
Phone 310 448-9449 FAX 310 823-6714**

Dan M. Davis

**HPC-Education
6275 E 6th St
Long Beach, California
dmdavis@acm.org
Phone: 310 909-3487**

Daniel P. Burns

**Home Ports Solutions, LLC
125 East 44th Street
Savannah GA 31405
nbr1cheng@prodigy.net
Phone: (831) 915-1212**

ABSTRACT

The Test and Evaluation (T&E) community is at the forefront of meeting the challenges presented by the cyber security attacks on U.S. infrastructure, industry and individuals. This requires a trained and agile response capability. While large cyber simulations are extant, e.g. Cyber Guard and Cyber Flag, they are costly, schedule-constrained and not easily tailored to small test environment requirements. There are clearly a range of many parameters of this problem: size, scope, and technologies. Work by personnel from the Information Sciences Institute of the University of Southern California, along with personnel from the California Air National Guard and a major National Laboratory, have developed a set of simulations and techniques for use by small cyber security units. These new approaches should be directly applicable to the T&E environment as well as to the training environment for which they were originally designed. The process consisted of the conception, design and implementation the Cyber Quick-Reaction Training Environment (CQRTE). This paper focuses on our research and development (R&D) efforts, which used HPC to stand up this low-cost fully operable simulated cyberspace environment. As best as can be ascertained, it is the first of its kind. The project has demonstrated how CQRTE can effectively model warfare principles within the context of cyberspace operations and, when implemented, these principles can achieve a valuable test environment. The designers recognized the necessity of having effective methods of capturing, logging, archiving and displaying the resultant data. This data management system will be useful if the CQRTE system were to be adopted for T&E use. The authors lay out the criticality of a high level approach to understanding which elements of the data need attention, as well as how to structure and visualize the data to produce insights that will otherwise go unnoticed. This paper describes how to assist technical personnel in their efforts to improve the testing of how the critical cyber threat is being met. It is also a paradigm case for organizational analysis driving data management design. The tactic of minimizing costs, facilitating access, and improving utility by using open source software is presented. The various parameters of the performance and the experience during the simulated cyber event will be offered and analyzed. The record of the first implementation of this process will be presented, along with the results of the first complete exercise using the system. The paper will close with an analysis of the utility of this approach, its extensibility into other areas, and future research requirements.

ABOUT THE AUTHORS

Ke-Thia Yao is a research scientist in the Computational Systems and Technology Division of the University of Southern California (USC) Information Sciences Institute (ISI). His primary research interest is helping people understand large complex systems and data sets. He has conducted data management research on the JESPP project with the goal of supporting very large-scale distributed military simulation involving millions of entities. Within the JESPP project he developed a suite of monitoring/logging/analysis tools to help users better understand the computational and behavioral properties of large-scale simulations. He received his B.S. degree in EECS from UC Berkeley, and his M.S. and Ph.D. degrees in Computer Science from Rutgers University.

John J. Tran is a Major in the California Air National Guard., where he focused on Object-oriented software engineering, large-scale software system design and implementation, and high performance parallel and scientific computing. He has worked at ISI, USC, the Stanford Linear Accelerator Center, Safetopia, and Intel Corporation. His current research centers on Linux cluster engineering, effective control of parallel programs, and communications fabrics for large-scale computation. His tours of duty included the White House Communications Agency and Kirkuk Regional Air Base (Iraq), where he was the Communications Squadron Commander. John is a PhD candidate in Computer Science at USC and is a programmer at the Aerospace Corporation. He received both his BS and MS Degrees in Computer Science and Engineering from the University of Notre Dame

Robert F. Lucas is a Deputy Director of the Information Sciences Institute at the University of Southern California and leads the Computational Sciences Division. He is a Research Associate Professor in the USC Department of Computer Science. At ISI he manages research in computer architectures, VLSI, compilers, and other software tools. He was the principal investigator on the JESPP project from 2002 to 2011, which first implemented GPU acceleration in high performance computing for battlefield simulations. Prior to joining ISI, he did tours as the Director of High Performance Computing Research for NERSC at LBNL, the Deputy Director of DARPA's ITO, and a researcher at the Institute for Defense Analyses, supporting the National Security Agency. Dr. Lucas earned BS, MS, and PhD degrees in Electrical Engineering from Stanford University.

Dan M. Davis was the JESPP project director at ISI, USC, where he now consults on distributed DoD simulations. Earlier, as Assistant Director of the Center for Advanced Computing Research at Caltech, he managed Synthetic Forces Express, bringing HPC to DoD battlefield simulations. Other positions include having been a Director at the Maui High Performance Computing Center and a Software Engineer at the Jet Propulsion Laboratory and Martin Marietta. He saw duty in Vietnam as a USMC Cryptologist and retired as a Commander, U.S.N.R. He holds B.A. and J.D. degrees from the University of Colorado.

Daniel P. Burns is a lifelong Systems Engineer first with the Active Duty Navy, then with a Fortune 250 Company and small business as well as in Academia. He formerly served as Naval Chair and a Professor of Practice in the Department of Systems Engineering at the Naval Postgraduate School (NPS) in Monterey California. He is a retired Captain in the United States Navy and has served as the Military Associate Dean and as acting Dean of the Graduate School of Engineering and Applied Sciences at NPS. For eight years he directed research as a senior executive at SAIC. His research interests center on analyses of both human and resource utilization in defense efforts. Captain Burns received a BS degree from the U.S. Naval Academy and an MS from the Naval Postgraduate School. He is currently finishing his dissertation for a PhD from Southern Methodist University.