

# IEEE Workshop on Visualization for Computer Security 2005 (VizSEC 05)

Minneapolis, Minnesota

October 26, 2005

## Proceedings

Edited by

Kwan-Liu Ma

Stephen North

Bill Yurcik



SPONSORED BY IEEE VISUALIZATION AND GRAPHICS TECHNICAL  
COMMITTEE (vgtc)

Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of US copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through:

Copyright Clearance Center  
222 Rosewood Drive  
Danvers, MA 01923

For other copying, reprint or republication permission, write to:  
IEEE Copyrights Manager  
IEEE Operations Center  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society Press, or the Institute of Electrical and Electronics Engineers, Inc.

ISBN: 0-7803-9477-1

Library of Congress Number: 2005932325

Additional copies may be ordered from the IEEE Service Center:  
IEEE Catalog Number: 05EX1205  
IEEE Operations Center  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331 USA

Telephone (toll-free): 1-800-678-IEEE  
Telephone (direct): +1-732-981-0060  
Fax: +1-732-981-9667  
E-mail: [customer-service@ieee.org](mailto:customer-service@ieee.org)

# Contents

Supporting Organizations .....	v
Preface.....	vi
IEEE Computer Society Technical Committee on Visualization and Graphics .....	vii
Organizers.....	viii
Program Committee.....	viii
Reviewers .....	viii

## Papers

### Session 1

Chair: Stephen North

IDS RainStorm: Visualizing IDS Alarms .....	3
Kulsoom Abdullah, Chris Lee, Gregory Conti, John A. Copeland and John Stasko	
Visual Correlation of Host Processes and Network Traffic .....	13
Glenn A. Fink, Paul Muessig and Chris North	
A User-centered Look at Glyph-based Security Visualization.....	23
Anita Komlodi, Penny Rheingans, Utkarsha Ayachit, John R. Goodall and Amit Joshi	
A Visualization Methodology for Characterization of Network Scans.....	31
Chris Muelder, Kwan-Liu Ma and Tony Bartoletti	

### Session 2

Chair: Kwan-Liu Ma

IDGraphs: Intrusion Detection and Analysis Using Histograms.....	41
Pin Ren, Yan Gao, Zhichun Li, Yan Chen and Benjamin Watson	
Preserving the Big Picture: Visual Network Traffic Analysis with TNV .....	49
John R. Goodall, Wayne G. Lutters, Penny Rheingans and Anita Komlodi	
Root Polar Layout of Internet Address Data for Security Administration .....	57
Glenn A. Fink and Chris North	
Visualization of Automated Trust Negotiation .....	67
Danfeng Yao, Michael Shin, Roberto Tamassia and William H. Winsborough	

### Session Short Papers

Chair: Bill Yurcik

Closing-the-Loop in NVisionIP: Integrating Discovery and Search in Security Visualizations .....	77
Kiran Lakkaraju, Ratna Bearavolu, Adam Slagell, William Yurcik and Stephen North	
Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries .....	85
Gregory Conti, Julian Grizzard, Mustaque Ahamad and Henry Owen	
Visualizing Cyber Attacks Using IP Matrix.....	93
Hideki Koike, Kazuhiro Ohno and Kanba Koizumi	
Multiple Coordinated Views for Network Attack Graphs .....	101
Steven Noel, Michael Jacobs, Pramod Kalapa and Sushil Jajodia	

Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned .....	109
Anita D'Amico and Michael Kocka	
Exploring Three-dimensional Visualization for Intrusion Detection .....	115
Adam Oline and Dirk Reiners	
Designing Visualization Capabilities for IDS Challenges .....	123
Robert F. Erbacher, Kim Christensen and Amanda Sundberg	
Visual Firewall: Real-time Network Security Monitor.....	131
Chris P. Lee, Jason Trost, Nicholas Gibbs, Raheem Beyah and John A. Copeland	
Author Index .....	Inside Back Cover

# Supporting Organizations

The conference and its affiliated symposia and workshops would like to sincerely thank the following organizations for their support:

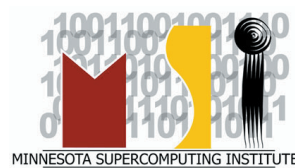
## Supporters Gold

---



## Supporters

---



## VizSEC 2005 Supporters

---



The world's networking company<sup>SM</sup>



# Preface

Computer security is one of the key problems of our day. Security operations analysts and researchers alike cope with difficult challenges in the scale and complexity of the data that must be analyzed to ensure the integrity of computer networks and systems.

VizSEC 2005 covers many leading research topics in the interdisciplinary area of visualization and human interfaces for computer security. The submitted papers show several noteworthy trends. We are glad to see that many practical prototype systems are converging and building off each other. Also, the program includes papers on two relatively new security visualization domains - firewall alert and trust negotiation. Several institutes have two accepted papers, and we have a first commercial VizSEC paper.

To be inclusive, we accepted more than 50% of the submissions. About 20% of the papers incorporate user studies, which is good to see. It seems appropriate that this year's VizSEC drew more of an emphasis on viz than security, given co-location between premiere visualization conferences. The program is still somewhat U.S.-centric; so further efforts are needed to reach a broader technical audience.

VizSEC 2005 is delighted to acknowledge the sponsorship of AT&T Labs and the National Science Foundation, as well as the strong support of the IEEE Technical Committee on Visualization and Graphics. We particularly thank Jenny Papenbrock, Steven Bergner, and Torsten Möller for their work on the proceedings.

Kwan-Liu Ma, Stephen North, and Bill Yurcik

## Mission

The IEEE Visualization and Graphics Technical Committee (VGTC) is a formal subcommittee of the Technical Activities Board (TAB) of the IEEE Computer Society. The VGTC provides technical leadership and organizes technical activities in the areas of visualization, computer graphics, virtual and augmented reality, and interaction.

The VGTC sponsors not only the annual Visualization and Virtual Reality conferences, but also many focused symposia and conferences, including InfoVis, Volume Graphics, Point-Based Graphics, and EuroVis (formerly VisSym).

## Awards

To recognize its members for their outstanding technical accomplishments, the VGTC sponsors a series of technical awards since 2004. The awards honor outstanding technical achievements in visualization and virtual reality. VGTC members may nominate individuals by contacting the awards chair, John Staudhammer, at <http://tab.computer.org/vgtc/>.

## VGTC Executive Committee

### Chair

Hanspeter Pfister  
MERL – Mitsubishi Electric  
Research Laboratories  
[pfister@merl.com](mailto:pfister@merl.com)

### Directors

Arie E. Kaufman  
Department of Computer Science  
State University of New York  
at Stony Brook  
[ari@cs.sunysb.edu](mailto:ari@cs.sunysb.edu)

### Bowen Loftin

Vice President and Chief Executive  
Officer  
Professor of Maritime Systems  
Engineering  
Texas A&M University at Galveston  
[loftin@tamug.edu](mailto:loftin@tamug.edu)

### Robert Moorhead

Visualization, Analysis,  
and Imaging Lab  
Mississippi State University  
[rjm@ERC.MsState.Edu](mailto:rjm@ERC.MsState.Edu)

### Gregory M. Nielson

Computer Science Department  
Arizona State University  
[nielson@asu.edu](mailto:nielson@asu.edu)

### vice chair for conferences

William Ribarsky  
Department of Computer Science  
University of North Carolina  
at Charlotte  
[ribarsky@uncc.edu](mailto:ribarsky@uncc.edu)

### liaison for national initiatives

Larry Rosenblum  
National Science Foundation  
[lrosenbl@nsf.gov](mailto:lrosenbl@nsf.gov)

### Appointed Officers

#### finance chair

Loretta Auvil  
National Center for  
Supercomputing Applications  
University of Illinois  
at Urbana Champaign  
[lauvil@ncsa.uiuc.edu](mailto:lauvil@ncsa.uiuc.edu)

#### web master

Dirk Bartz  
Computer Graphics Lab  
University of Tübingen  
[bartz@gris.uni-tuebingen.de](mailto:bartz@gris.uni-tuebingen.de)

#### international liaison

Hans Hagen  
Computer Science Department  
Technical University of Kaiserslautern  
[hagen@informatik.uni-kl.de](mailto:hagen@informatik.uni-kl.de)

#### secretary

Elizabeth Jurrus  
Scientific Computing  
and Imaging Institute  
University of Utah  
[liz@cs.utah.edu](mailto:liz@cs.utah.edu)

## National Initiatives

The VGTC is actively involved in national initiatives that study and promote the immediate and long-range challenges in visualization and computer graphics and related research areas. For more information visit our web page.

## Getting Involved

Membership in the VGTC is open to all individuals interested in visualization and computer graphics at a professional level. There are no dues for VGTC membership and no IEEE membership requirements.

## Web Site

Visit the VGTC web site at <http://tab.computer.org/vgtc>. It offers information about how to join, VGTC activities, awards, national initiatives, conferences and symposia, and contains a link to a comprehensive membership directory.

Hanspeter Pfister VGTC Chair

### publication chair

Torsten Möller  
School of Computing Science  
Simon Fraser University  
[vis@cs.sfu.ca](mailto:vis@cs.sfu.ca)

### Members at Large

John C. Dill  
EIC IEEE CG&A  
School of Engineering Science  
Simon Fraser University  
[dill@cs.sfu.ca](mailto:dill@cs.sfu.ca)

### David Ebert

EIC IEEE TVCG  
School of Electrical and  
Computer Engineering  
Purdue University  
[ebertd@ecn.purdue.edu](mailto:ebertd@ecn.purdue.edu)

### Eduard Gröller

Institute of Computer Graphics  
and Algorithms  
Vienna University of Technology  
[groeller@cg.tuwien.ac.at](mailto:groeller@cg.tuwien.ac.at)

### Victoria Interrante

Department of Computer Science  
and Engineering  
University of Minnesota  
[interran@cs.umn.edu](mailto:interran@cs.umn.edu)

### Daniel A. Keim

Computer Science Institute  
University of Konstanz  
[keim@informatik.uni-konstanz.de](mailto:keim@informatik.uni-konstanz.de)

### Tamara Munzner

Computer Science Department  
University of British Columbia  
[tmm@cs.ubc.ca](mailto:tmm@cs.ubc.ca)

### Penny Rheingans

Department of Computer Science  
and Electrical Engineering  
University of Maryland,  
Baltimore County  
[rheingan@cs.umbc.edu](mailto:rheingan@cs.umbc.edu)

### Randall C. Smith

Vehicle Development Research Lab  
General Motors Research  
& Development  
[randall.c.smith@gm.com](mailto:randall.c.smith@gm.com)

### Jim Thomas

Pacific Northwest National  
Laboratory  
U.S. Department of Energy  
[jim.thomas@pnl.gov](mailto:jim.thomas@pnl.gov)

### Ben Watson

Department of Computer Science  
Northwestern University  
[watson@northwestern.edu](mailto:watson@northwestern.edu)

## Organizers

---

### Workshop Chair

Kwan-Liu Ma  
University of California at Davis

### Program Co-Chairs

Stephen North  
AT&T Labs

Bill Yurcik  
NCSA

## Program Committee

---

Tony Bartoletti  
Lawrence Livermore National  
Laboratory

Baoquan Chen  
University of Minnesota

Gregory Conti  
Georgia Institute of Technology

Stephen Eick  
University of Illinois-Chicago & SSS  
Research

Robert Erbacher  
Utah State University

Emden Gansner  
AT&T Labs

Tom Goldring  
US National Security Agency

John Goodall  
University of Maryland at Baltimore  
County

T. J. Jankun-Kelly  
Mississippi State University

Daniel Keim  
University of Konstanz, Germany

Hideki Koike  
University of Electro-Communica-  
tions

Tamara Munzner  
University of British Columbia

Klaus Mueller  
Stony Brook University

Chris North  
Virginia Polytechnic Institute and  
State University

Penny Rheingans  
University of Maryland at Baltimore  
County

William Ribarsky  
University of North Carolina at  
Charlotte

Richard Strelitz  
Los Alamos National Laboratory

Roberto Tamassia  
Brown University

Soon Tee Teoh  
University of California at Davis

Walt Tirenin  
Air Force Research Laboratory

Vivek Verma  
Sarnoff Corporation

Kirsten Whitley  
US Department of Defense

Pak Chung Wong  
Pacific Northwest National Labora-  
tory

## Reviewers

---

Kulsoom Abdullah  
Tony Bartoletti  
Steven Bellovin  
Susan Bridges  
Baoquan Chen  
Gregory Conti  
Carlos Correa  
Julie Dickerson  
Stephen Eick  
Niklas Elmqvist  
Robert Erbacher  
Glenn Fink  
Emden Gansner  
Alexander Gee

Tom Goldring  
John Goodall  
Denis Gracanin  
Donna Gresh  
Eric Harder  
T. J. Jankun-Kelly  
Daniel Keim  
Hideki Koike  
Paul Krystosek  
Kiran Lakkaraju  
Robert Edward Loke  
Toshiyuki Masui  
Patrick McCormick  
Patrick McDaniel

Peter McLachlan  
Jörg Meyer  
Klaus Mueller  
Tamara Munzner  
Chris North  
Stephen North  
Penny Rheingans  
William Ribarsky  
Gerik Scheuermann  
Colleen Shannon  
Richard Sharp  
Steve Smith  
Richard Strelitz  
Tetsuji Takada

Roberto Tamassia  
Diane Tang  
Soon Tee Teoh  
Walt Tirenin  
Vivek Verma  
Kirsten Whitley  
Sarah Winter  
Pak Chung Wong  
Xiaoru Yuan  
William Yurcik