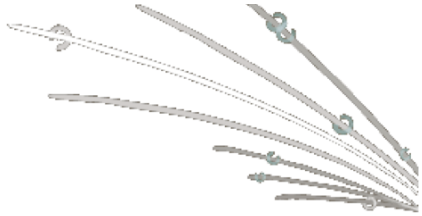
VizSec 2009

Workshop on Visualization for Cyber Security

October 11, 2009 / Atlantic City, NJ USA
http://vizsec.org/vizsec2009/



Call For Participation

Goals

The 6th International Workshop on Visualization for Cyber Security is a forum that brings together researchers and practitioners in information visualization and security to address the specific needs of the cyber security community through new and insightful visualization techniques. Co-located this year with IEEE InfoVis/Vis/VAST, VizSec will continue to provide opportunities for the two communities to collaborate and share insights into providing solutions for security needs through visualization approaches. Accepted papers will be published by the IEEE and archived in the IEEE Digital Library. The authors of the best papers will be invited to extend and revise their paper for journal publication in a special issue of *Information Visualization*.

This year our focus is on advancing Visualization for Cyber Security as a scientific discipline. While art, engineering, and intuitions regarding the human element will always remain important if we are to obtain useful cyber security visualizations, advances in the scientific practice of research are needed. The scientific aspects of visualization for cyber security draw both on empirical observation (similar to many natural and social sciences) and formal science (such as the formal derivations in mathematics). Barriers confronting current researchers include concerns about available data, lack of a common agreement about what constitutes sound experimental design, the difficulties of measuring the relative effectiveness of security visualizations in practice, and the lack of a common understanding of user requirements. While many researchers are making progress in these and other critical areas, much work yet remains.

How to Submit

http://www.vizsec.org/vizsec2009/submit

Important Dates

Full papers due:	24 April 2009 11:59pm PDT
Short papers due:	22 May 2009 11:59pm PDT
Author notification:	5 June 2009
Camera-ready copies:	26 June 2009

What To Submit

Papers offering novel contributions in security visualization are solicited. Papers may present technique, applications, practical experience, theory, or experiments and evaluations. Papers are encouraged on technologies and methods that have been demonstrated to be useful for improving information systems security and that address lessons from actual application. We encourage papers that report results on visualization techniques and systems in solving all aspects of cyber security problems, including how visualization applies to:

- Different aspects of security: software, networks and log files (e.g., Internet routing, packet traces and network flows, intrusion detection alerts, attack graphs, application security, etc.)
- Application of visualization techniques in formalizing, defining and analyzing security policies
- Forensic analysis, correlating events, cyber-defense task analysis
- Computer network defense training and offensive information operations
- Building rules, feature selection, and detecting anomalous activity
- Software, software security, and viruses
- Deployment and field testing of VizSec systems
- Evaluation and user testing of VizSec systems
- User and design requirements for VizSec systems
- Lessons learned from development and deployment of VizSec systems
- "Field Research" Best Practices
- Interaction with domain experts – best practices, lessons learned
- Differentiating the needs of different domains and time frames
- Best practices for obtaining and sharing potentially sensitive data for purposes of visualization and assessment, including how to approach personal privacy, regulatory, and organizational issues
- Metrics and measurements (e.g., criteria for the relative effectiveness of cyber visualizations)
- Handling large datasets, scalability issues, and providing real time or near-real time visualizations

Accepted papers will be published by the IEEE and made available through the IEEE Digital Library.

Paper Format

Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. All submissions should be appropriately anonymized (i.e., papers should not contain author names or affiliations, or obvious citations). Submissions are to be made to the submission web site at http://www.vizsec.org/vizsec2009/submit. Only pdf files will be accepted. Papers should be formatted using the IEEE templates (see http://www.vizsec.org/vizsec2009/ for instructions).

- Full papers should be at most 12 pages, including the bibliography and appendices.
- Short papers should be at most 6 pages, including the bibliography and appendices.

Committee members are not required to read the appendices, and so the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits. Authors of accepted papers must guarantee that their papers will be presented at the conference.

Papers must be received by the deadline of April 24, 2009, for long papers and May 22, 2009, for short papers.

Journal Special Issue

The authors of the best papers from the accepted program will be invited to extend and revise their paper for a special issue of *Information Visualization* (IVS), an international, peer-reviewed journal publishing articles on fundamental research and applications of information visualization. These papers will be chosen by the program committee.

Paper Award

There will be an award for the best paper from the accepted program. The best paper award will be given to the paper judged to have the highest overall quality. A key element of the best paper selection process will be whether the results are believed to be repeatable by other scientists based on the algorithms and data provided in the paper. This award will be chosen by the program committee.

Scholarships

A limited number of scholarships will be available for students and first-year faculty who have had papers accepted to VizSec.

Organizing Committee

General Chair	Deborah Frincke, Pacific Northwest National Laboratory and University of Washington
Program Co-Chair:	Carrie Gates, CA Labs
Program Co-Chair:	John Goodall, Secure Decisions Division of Applied Visions
Papers Chair:	Robert Erbacher, Utah State University

Program Committee

Richard Beijtich, General Electric, USA
Greg Conti, United States Military Academy, USA
Marc Dacier, Symantec Research Labs, France
Anita D'Amico, Secure Decisions div. of Applied Visions, USA
Ron Dilley, Information Security Professional, USA
Dave Ebert, Purdue University, USA
Glenn Fink, Pacific Northwest National Lab, USA
John Gerth, Stanford University, USA
Warren Harrop, Swinburne Univ. of Technology, Australia
Mark Haselkorn, University of Washington, USA
Richard Johnson, Microsoft, USA
Richard Kemmerer, UC Santa Barbara, USA
Toby Kohlenberg, Intel, USA
Florian Mansmann, University of Konstanz, Germany
Raffael Marty, Splunk, USA
Doug Maughan, Department of Homeland Security, USA
John McHugh, Dalhousie Univ., Canada, and Univ. NC, USA
Jan P. Monsch, Dublin City University, Ireland
Chris North, Virginia Tech, USA
Stephen North, AT&T Research, USA
Sean Peisert, UC Davis, USA
Greg Schmidt, SPADAC, USA
George Tadda, Air Force Research Lab, USA
Ed Talbot, Sandia National Laboratories, USA
Joanne Treurniet, Defence R&D Canada, Canada
Grant Vandenberghe, Defence R&D Canada, Canada
Kirsten Whitley, Department of Defense, USA
Pak Chung Wong, Pacific Northwest National Lab, USA
Tamara Yu, Massachusetts Institute of Technology, USA

http://vizsec.org/vizsec2009/