VizSec2010

Symposium on Visualization for Cyber Security

September 14, 2010 / Ottawa, Ontario, Canada

In conjunction with RAID 2010.

The International Symposium on Visualization for Cyber Security (VizSec) is a forum that brings together researchers and practitioners in information visualization and cyber security to address the specific needs of the cyber security community through new and insightful visualization techniques. Co-located this year with Symposium on Recent Advances in Intrusion Detection (RAID), the 7th 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 appear in the ACM Digital Library as part of the ACM International Conference Proceedings Series.

This year our focus is on understanding what makes effective visual interfaces for different cyber security tasks. This involves both advancing our understanding of what cyber security tasks are, and improving our understanding of what it means for a security visualization to be effective. Cyber security visualization tasks cover a wide range, including (but not limited to) acquiring situational awareness in massive datasets; analyzing data from disparate sources during incident handling; producing actionable reports for others; modeling the behavior of systems; and predicting future events. Understanding the effectiveness of a cyber security visualization is not limited only to the usability of the interface itself, but, perhaps even more importantly, to the assessment of how the visualization advances security goals. Barriers confronting current researchers include understanding the tasks where visualization can be effective, concerns about available data for both usability and effectiveness assessment, lack of a common agreement about what constitutes sound experimental design, and the difficulties of measuring the relative effectiveness of security visualizations in practice. Additionally, discussions at VizSec 2009 raised the question about what role a science-based approach ought to play in the conjunction of visualization and security. While many researchers are making progress in these and other critical areas, much work remains.

Technical Papers

Full and short papers, poster abstracts and panel abstracts 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:

- Situational awareness/understanding
- Incident handling including triage, exploration, correlation, and response
- Recording and reporting results of investigation
- Modeling system and network behavior
- Criteria for assessing the effectiveness of cyber security visualizations (whether from a security goal perspective or a human factors perspective)
- Predicting future attacks or targets
- Evaluation/user testing of VizSec systems
- Lessons learned
- Privacy considerations for managing VizSec data

Accepted papers and abstracts will appear in the ACM Digital Library. The program committee will select an accepted paper to receive the VizSec 2010 best paper award. 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.

It is anticipated that authors of the best papers will be invited to extend and revise their paper for journal publication in a special issue, as in previous years.

Paper formatting and submission instructions are on the VizSec 2010 web site:
http://www.vizsec2010.org/

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.
Poster and panel abstracts should be 2 pages, including the bibliography and appendices.

Committee members are not required to read the appendices, or any pages past the maximum. Submissions not meeting these guidelines will be rejected without consideration of their merits. Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Authors of accepted papers must guarantee that their papers will be presented at the conference, preferably by themselves or by prior arrangement through a delegate.

Dates

Technical papers:

4/30/2010	Full paper submissions
5/21/2010	Short paper submissions
6/17/2010	Notification to all paper authors
7/30/2010	Final camera-ready version of all papers due

Posters:

7/23/2010	Poster abstract submissions (final, camera-ready version)
7/30/2010	Notification to poster authors

Panels:

6/11/2010	Panel abstract submissions
7/9/2010	Notification to panel organizers
7/30/2010	Final camera ready version of panel abstract

Scholarships

A limited number of scholarships may be available for students and first-year faculty who have had papers accepted to VizSec in the form of a fee waiver or small honorarium. The number of scholarships actually available will be dependent on VizSec sponsorship and meeting costs.

Organizing Committee

General Chair:	John Gerth, Stanford University
Emeritus Chair:	Deb Frincke, Pacific Northwest National Laboratory
Program Chair:	Dino Schweitzer, US Air Force Academy
Publication Chair:	John Goodall, Secure Decisions division of Applied Visions Inc.

http://www.vizsec2010.org/