Association for Computing Machinery

ACM International Conference Proceedings Series

VizSec 2010

Proceedings of the Seventh International Symposium on Visualization for Cyber Security

Ottawa, Ontario, Canada
September 14, 2010

http://vizsec2010.org/

Sponsored By:

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

APPLIED VISIONS SecureDecisions DIVISION

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York, New York 10121-0701

ISBN: 978-1-4503-0013-1

Forward

Welcome to Ottawa and VizSec 2010, the International Symposium on Visualization for Cyber Security. This year represents the seventh meeting of researchers, practitioners, and educators interested in the application of visualization techniques to the critical area of cyber security. This year, VizSec is being held in conjunction with the International Symposium on Recent Advanced in Intrusion Detection (RAID). Security visualization and intrusion detection are two aspects of cyber security that are well suited for each other. Both deal with huge amounts of data, the need to analyze and understand the data for critical decision-making, and, often, the requirement to do so in near-real time.

Since VizSec's inception in 2004, many advances have been made in the development of tools and techniques for visualizing security-related data. Initially, much of the work was applying existing tools from the visualization community, or simply treating security as another application area. However, some of the unique requirements of cyber security: the huge amounts of data such as network traffic, the need for near-real time decisions when monitoring systems, and the possible incomplete or conflicting data when dealing with forensics have led to new approaches and techniques. In addition, security visualization has a large human component in the usability and effectiveness of techniques when applied in operational environments. VizSec continues to be a blend of research and application across a wide variety of security topics.

This year we received 27 technical paper submissions. Each paper was refereed by at least three members of the program committee, which selected twelve papers for inclusion in the program and symposium proceedings. This year's papers reflect the diversity of the symposium and field. Traditional areas such as new approaches to network visualization and intrusion detection are combined with visualization techniques for secure code and secure phone calls. Management issues such as situational awareness and incident management are also addressed. New hardware capabilities are reflected in a paper on the application of a multi-touch user interface to cyber security. Our keynote speaker, Richard Bejtlich, addresses the utility of security visualization in production systems.

We would like to thank the paper authors, members of the program committee, and the organizing committee. Thanks to our sponsor, National Information Assurance Research Laboratory, and to Applied Visions, Inc. – Secure Decisions Division for sponsoring the proceedings USB drives. We would also like to thank Communications Research Centre Canada for hosting VizSec and ACM for publishing our proceedings in the ACM Digital Library as part of the ACM International Conference Proceedings Series.

John Gerth
General Chair
Stanford University

Dino Schweitzer
Program Chair
U.S. Air Force Academy

John R. Goodall
Publications Chair
Oak Ridge National Lab

VizSec 2010 Organization

General Chair: John Gerth, Stanford University

Emeritus Chair: Deb Frincke, Pacific Northwest National Laboratory

Program Chair: Dino Schweitzer, United States Air Force Academy

Publication Chair: John R. Goodall, Oak Ridge National Laboratory

Local Chair: Grant Vandenberghe, Defence Research and Development Canada

Local Co-Chair: Frédéric Massicotte, Communications Research Centre Canada

Program Committee:

David Barrera, Carleton University
Richard Bejtlich, General Electric
Carter Bullard, QoSient, LLC
Bill Cheswick, AT&T Research
Marc Dacier, Symantec Research Labs
Ron Dilley, Warner Bros.
David Ebert, Purdue University
Alex Endert, Virginia Tech
Rob Erbacher, Utah State University
Carrie Gates, CA Labs
Joel Glanfield, Dalhousie University
Warren Harrop, Swinburne University of Technology
Aidong Lu, UNC Charlotte
Florian Mansmann, University of Konstanz
Raffael Marty, Loggly
Doug Maughan, Homeland Security
Jan Monsch, Google
Stephen North, AT&T
Danny Quist, Offensive Computing
Mike Sips, Max Planck Institut Informatik
Teryl Taylor, Dalhousie University
Joanne Treurniet, Defence Research and Development Canada
Rick Wesson, Support Intelligence
Kirsten Whitley, Department of Defense
Pak Chung Wong, Pacific National Laboratory
Anatoly Yelizarov, Moscow State University
Tamara Yu, MIT Lincoln Laboratory

Table of Contents

VizSec 2010 Program

7:30 – 8:45 Breakfast and Registration

8:45 - 9:00 Welcome: John Gerth, VizSec General Chair

9:00 – 10:00 Keynote: Richard Bejtlich, General Electric
Is Security Visualization Useful in Production?

10:00 – 10:30 Health Break

10:30 – 12:00 Paper Session 1

EMBER: A Global Perspective on Extreme Malicious Behavior
Tamara Yu, Richard Lippmann, James Riordan, Stephen Boyer

Proposing a Multi-touch Interface for Intrusion Detection Environments
Jeffrey Guenther, Fred Volk and Mark Shaneck

Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR *
Matthew Chu, Kyle Ingols, Richard Lippmann, Seth Webster and Stephen Boyer

Visualizing Graph Dynamics and Similarity for Enterprise Network Security and Management *
Qi Liao, Aaron Striegel and Nitesh Chawla

12:00 – 13:30 Lunch and Technology Showcase

13:30 – 14:30 Paper Session 2

Visual Analysis of Code Security
John R. Goodall, Hassan Radwan, Lenny Halseth

PeekKernelFlows: Peeking into IP flows
Cynthia Wagner, Gerard Wagener, Radu State, Alexandre Dulaunoy and Thomas Engel

Visualizing Host Traffic through Graphs
Eduard Glatz

Visualizing Your Key for Secure Phone Calls And Language Independence *
Michael Oehler, Dhananjay Phatak and John Krautheim

14:30 – 15:00 Health Break

15:00 – 16:30 Paper Session 3

Traffic Classification Using Visual Motifs: An Empirical Evaluation
Wilson Lian, Fabian Monrose and John McHugh

Real-Time Visualization of Network Behaviors for Situational Awareness
Daniel Best, Shawn Bohn, Douglas Love, Adam Wynne and William Pike

Interactive Detection of Network Anomalies via Coordinated Multiple Views
Lane Harrison, Xianlin Hu, Xiaowei Ying, Aidong Lu, Weichao Wang and Xintao Wu

Nimble Cybersecurity Incident Management through Visualization and Defensible Recommendations *
Jamie Rasmussen, Kate Ehrlich, Steven Ross, Susanna Kirk, Daniel Gruen and John Patterson

18:00 – 20:00 Reception, Poster Session and Technology Showcase

* Best paper nominee.

Posters

A Visual Query Builder: Simplifying Data Selection

Robert Ferris and John R. Goodall

Collaborative Multitouch Log Browsing

Jeff Wilson and Robert Biddle

Graphical Passwords Using Google Maps

Jake Spitzer and Cal Singh

Detecting Cloned Portions of Images

Steven Glowacki and Joshua Gminski

The Need to Support of Data Flow Graph Visualization of Forensic Lucid Programs, Forensic Evidence, and their Evaluation by GIPSY

Serguei Mokhov, Joey Paquet and Mourad Debbabi

Keynote Presentation

Richard Bejtlich, General Electric – *Is Security Visualization Useful in Production?*

Is there is a disconnect between security visualization in theory and practice? In this keynote, Richard Bejtlich will discuss the strengths and weaknesses of using security visualization in the enterprise. For example, why do analysts consistently refer to traditional displays, despite nearly ten years of work in the visualization arena? Why are most security products so limited when rendering data? What must be done to change this situation? Richard will explore these topics based on experiences as Principal Technologist and Director of Incident Response for General Electric.

Richard Bejtlich is Director of Incident Response for General Electric, and serves as Principal Technologist for GE's Global Infrastructure Services division. Prior to GE, Richard operated TaoSecurity LLC as an independent consultant, protected national security interests for ManTech Corporation's Computer Forensics and Intrusion Analysis division, investigated intrusions as part of Foundstone's incident response team, and monitored client networks for Ball Corporation. Richard began his digital security career as a military intelligence officer at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. He wrote "The Tao of Network Security Monitoring" and "Extrusion Detection", and co-authored "Real Digital Forensics". He also writes for his blog (taosecurity.blogspot.com) and TechTarget.com, and teaches for Black Hat.