ACM COPYRIGHT NOTICE. Copyright © 2012 by the Association for Computing Machinery, Inc. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Publications Dept., ACM, Inc., fax +1 (212) 869-0481, or permissions@acm.org.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, +1-978-750-8400, +1-978-750-4470 (fax).

Notice to Past Authors of ACM-Published Articles
ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that was previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-1413-8
Forward

Welcome to VizSec 2012! VizSec is the International Symposium on Visualization for Cyber Security and is a forum that brings together researchers and practitioners from academia, government, and industry to address the needs of the cyber security community through new and insightful visualization techniques. This year, we are pleased to be a part of VisWeek, the premier forum for advances in scientific and information visualization. There is a wonderful synergy with being held along with VisWeek; it is the cutting edge tools and ideas presented at VisWeek that become the fuel for inspiration for visualizing critical cyber security issues.

Increasingly, cyber security plays a critical role in the health and well-being of nations around the world. Cyber-warfare, cyber-crime, and cyber-terrorism threaten the economic and political stability of modernized society. Massive botnets and automated attacks disrupt services, threaten national infrastructures, and fuels international crime. Visualization serves as a powerful tool to monitor, detect, and analyze security-related incidents. Whether providing a real-time view of network traffic and potential threats, or analyzing digital forensic data for attribution, visualization techniques can provide insights and understandings that are not gleaned from using traditional approaches. It is the combination of researching new visual approaches and evaluating the practical application of those techniques to real-world problems that is the heart of VizSec.

This year we received 21 technical paper submissions. Each paper was refereed by three members of the program committee, which selected twelve papers for inclusion in the program and proceedings. This year's papers once again reflect the diversity of the field. Low level topics such as analyzing distributed memory computations and firewall configurations are mixed with higher level issues such as designing visualizations to provide situational awareness capability. Our keynote speaker, Raphael Marty, is a well-known advocate and practitioner of security visualization who has for many years hosted an informative forum for sharing ideas and experiences in the practical aspects of employing visualization principles to cyber security.

An event like VizSec does not happen in a vacuum. We would very much like to thank the paper authors, members of the program committee, and the organizing committee for their time and dedication to this endeavor. We would also like to thank VisWeek for hosting us and ACM for publishing our proceeding in the ACM Digital Library as part of the ACM International Conference Proceedings Series.

Dino Schweitzer  
Chair  
U.S. Air Force Academy

Danny Quist  
Program Chair  
MIT Lincoln Laboratory

John R. Goodall  
Publications Chair  
Oak Ridge National Laboratory
VizSec 2012 Organization

Organizing Committee

General Chair    Dino Schweitzer, United States Air Force Academy
Program Chair    Daniel Quist, MIT Lincoln Laboratory
Publication Chair John R. Goodall, Oak Ridge National Laboratory

Program Committee

David Barrera, Carleton University
Daniel Best, Pacific Northwest National Laboratory
Richard Bejtlich, TaoSecurity
Greg Conti, US Military Academy at West Point
Ron Dilley, UberAdmin
David Ebert, Purdue University
Alex Endert, Virginia Tech
Rob Erbacher, Army Research Laboratory
Carrie Gates, CA Technologies
John Gerth, Stanford University
Mark Haselkorn, University of Washington
Tyler Hudak, KoreLogic Security
Kohlhammer Jörn, Fraunhofer IGD
Florian Mansmann, Universität Konstanz
Raffael Marty, PixlCloud
Jan Monsch, Google
Joe Parry, Cambridge Intelligence
Stephen North, AT&T
Teryl Taylor, University of North Carolina
Olivier Thonnard, Symantec
Joanne Treurniet, Defence Research and Development Canada
Kirsten Whitley, Department of Defense
Pak Chung Wong, Pacific Northwest National Laboratory
Anatoly Yelizarov, Lomonosov Moscow State University
Tamara Yu, MIT Lincoln Laboratory
# Table of Contents

Forward ....................................................................................................................... iii

Vizsec 2012 Organization ............................................................................................ iv

Keynote Presentation .................................................................................................. vi

**Visual Analysis of Complex Firewall Configurations**  
Florian Mansmann, Timo Göbel and William Cheswick ............................................ 1

**Automated Tracing and Visualization of Software Security Structure and Properties**  
Wenbin Fang, Barton P. Miller and James A. Kupsch ............................................... 9

**Visualization Design for Immediate High-Level Situational Assessment**  
Robert Erbacher ........................................................................................................ 17

**NV: Nessus Vulnerability Visualization for the Web**  
Lane Harrison, Riley Spahn, Mike Iannacone, Evan Downing and John R. Goodall .... 25

**Visualization of Shared System Call Sequence Relationships in Large Malware Corpora**  
Joshua Saxe, David Mentis and Chris Greamo ......................................................... 33

**MalwareVis: Entity-based Visualization of Malware Network Traces**  
Wei Zhuo and Yacin Nadji ......................................................................................... 41

**Change-Link: A Digital Forensic Tool for Visualizing Changes to Directory Trees**  
Timothy Leschke and Alan Sherman .......................................................................... 48

**Visualizing Distributed Memory Computations with Hive Plots**  
Sophie Engle and Sean Whalen ................................................................................ 56

**Visual Spam Campaigns Analysis using Abstract Graphs Representation**  
Orestis Tsigkas, Olivier Thonnard and Dimitrios Tzovaras ....................................... 64

**DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System**  
Daisuke Inoue, Koei Suzuki, Mio Suzuki, Masashi Eto and Koji Nakao ......................... 72

**VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes**  
Fabian Fischer, Johannes Fuchs, Pierre-Antoine Vervier, Florian Mansmann and Olivier Thonnard ................................................................. 80

**Visualizing Semantics in Passwords: The Role of Dates**  
Rafael Veras, Julie Thorpe and Christopher Collins .................................................. 88
Keynote Presentation

Raffael Marty: “Security Visualization - Let's Take a Step Back”

Raffael Marty is a SaaS business expert, data visualization practitioner, and security data analyst. Raffael is the founder and CEO of pixlcloud, a visual analytics company. Prior, he co-founded Loggly, a cloud-based log management company. He has been a long term data analysis and visualization enthusiast and has spent a lot of time building and defining the security visualization space through open source tools, writing books, a number of papers, and speaking at conferences around the world. He is frequently consulting as an industry expert in all aspects of log analysis, computer security, and data visualization.

Raffy has held various positions in the log management space at companies like Splunk, ArcSight, and IBM research where he also earned his masters in computer science. In addition to visualization, big data analysis, and computer security, Raffy is working with a number of startups and finds peace in zen meditation.