

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

John R. Goodall Gregory Conti
Kwan-Liu Ma (Eds.)

Visualization for Computer Security

5th International Workshop, VizSec 2008
Cambridge, MA, USA, September 15, 2008
Proceedings



Springer

Volume Editors

John R. Goodall
Secure Decisions division of Applied Visions
Albany, NY, USA
E-mail: johng@securedecisions.avi.com

Gregory Conti
United States Military Academy
West Point, NY, USA
E-mail: gregory.conti@usma.edu

Kwan-Liu Ma
University of California
Davis, CA, USA
E-mail: ma@cs.ucdavis.edu

Library of Congress Control Number: 2008934071

CR Subject Classification (1998): C.2, K.6.5, I.3, H.3.3, I.5.3

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-85931-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85931-4 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12515677 06/3180 5 4 3 2 1 0

Preface

This volume contains the papers presented at VizSec 2008, the 5th International Workshop on Visualization for Cyber Security, held on September 15, 2008 in Cambridge, Massachusetts, USA. VizSec 2008 was held in conjunction with the 11th International Symposium on Recent Advances in Intrusion Detection (RAID).

There were 27 submissions to the long and short paper categories. Each submission was reviewed by at least 2 reviewers and, on average, 2.9 program committee members. The program committee decided to accept 18 papers.

The program also included an invited talk and a panel. The keynote address was given by Ben Shneiderman, University of Maryland at College Park, on the topic Information Forensics: Harnessing Visualization to Support Discovery. The panel, on the topic The Need for Applied Visualization in Information Security Today, was organized and moderated by Toby Kohlenberg from Intel Corporation.

July 2008

John R. Goodall

Conference Organization

Program Chairs

John R. Goodall	Secure Decisions division of Applied Visions
Gregory Conti	United States Military Academy
Kwan-Liu Ma	University of California at Davis

Program Committee

Stefan Axelsson	Blekinge Institute of Technology
Richard Bejtlich	General Electric
Kris Cook	Pacific Northwest National Laboratory
David Ebert	Purdue University
Robert Erbacher	Utah State University
Deborah Frincke	Pacific Northwest National Laboratory
Carrie Gates	CA Labs
John Gerth	Stanford University
Barry Irwin	Rhodes University
Daniel Keim	University of Konstanz
Toby Kohlenberg	Intel Corporation
Stuart Kurkowski	Air Force Institute of Technology
Kiran Lakkaraaju	University of Illinois at Urbana-Champaign
Raffael Marty	Splunk
Douglas Maughan	Department of Homeland Security
John McHugh	Dalhousie University
Penny Rheingans	UMBC
Lawrence Rosenblum	National Science Foundation
George Tadda	Air Force Research Lab
Daniel Tesone	Applied Visions
Alfonso Valdes	SRI International
Kirsten Whitley	Department of Defense

Local Organization

Robert K. Cunningham	Lincoln Laboratory
----------------------	--------------------

Table of Contents

Visual Reverse Engineering of Binary and Data Files	1
<i>Gregory Conti, Erik Dean, Matthew Sinda, and Benjamin Sangster</i>	
Effective Visualization of File System Access-Control	18
<i>Alexander Heitzmann, Bernardo Palazzi, Charalampos Papamanthou, and Roberto Tamassia</i>	
Visual Analysis of Program Flow Data with Data Propagation.....	26
<i>Ying Xia, Kevin Fairbanks, and Henry Owen</i>	
A Term Distribution Visualization Approach to Digital Forensic String Search	36
<i>Moses Schwartz and L.M. Liebrock</i>	
GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool.....	44
<i>Leevar Williams, Richard Lippmann, and Kyle Ingols</i>	
A Graph-Theoretic Visualization Approach to Network Risk Analysis... ..	60
<i>Scott O'Hare, Steven Noel, and Kenneth Prole</i>	
Improving Attack Graph Visualization through Data Reduction and Attack Grouping	68
<i>John Homer, Ashok Varikuti, Xinming Ou, and Miles A. McQueen</i>	
Show Me How You See: Lessons from Studying Computer Forensics Experts for Visualization.....	80
<i>T.J. Jankun-Kelly, Josh Franck, David Wilson, Jeffery Carver, David Dampier, and J. Edward Swan II</i>	
A Task Centered Framework for Computer Security Data Visualization	87
<i>Xiaoyuan Suo, Ying Zhu, and Scott Owen</i>	
BGPeep: An IP-Space Centered View for Internet Routing Data	95
<i>James Shearer, Kwan-Liu Ma, and Toby Kohlenberg</i>	
Large-Scale Network Monitoring for Visual Analysis of Attacks	111
<i>Fabian Fischer, Florian Mansmann, Daniel A. Keim, Stephan Pietzko, and Marcel Waldvogel</i>	
Visualizing Real-Time Network Resource Usage.....	119
<i>Ryan Blue, Cody Dunne, Adam Fuchs, Kyle King, and Aaron Schulman</i>	

Wireless Cyber Assets Discovery Visualization	136
<i>Kenneth Prole, John R. Goodall, Anita D. D'Amico, and Jason K. Kopylec</i>	
NetFlow Data Visualization Based on Graphs	144
<i>Pavel Minarik and Tomas Dymacek</i>	
Backhoe, a Packet Trace and Log Browser	152
<i>Sergey Bratus, Axel Hansen, Fabio Pellacini, and Anna Shubina</i>	
Existence Plots: A Low-Resolution Time Series for Port Behavior Analysis	161
<i>Jeff Janies</i>	
Using Time Series 3D AlertGraph and False Alert Classification to Analyse Snort Alerts	169
<i>Shahruhniza Musa and David J. Parish</i>	
Network Traffic Exploration Application: A Tool to Assess, Visualize, and Analyze Network Security Events	181
<i>Grant Vandenberghe</i>	
Author Index	197