IEEE Symposium on Computational Intelligence in Cyber Security

(CICS 2009)

Nashville, Tennessee, USA
30 March – 2 April 2009

IEEE Catalog Number: CFP09CIY-PRT
ISBN: 978-1-4244-2769-7

TABLE OF CONTENTS

Tutorial CICS-T: Computational Intelligence in Cyber Security
Tuesday, March 31, 2:00PM-4:00PM, Room: Kingsley, Instructor: Dipakar Dasgupta, University of Memphis, USA

Session CICS-1: Network Attacks: analysis and detection
Wednesday, April 1, 8:30AM-10:30AM, Room: Belmont, Chair: Dipankar Dasgupta, University of Memphis, USA

Visualization of Network Components for Attack Analysis [#5] *1*

Hoin Kim, Inyong Lee, Jaeik Cho and Jongsub Moon

Center for Information Security Technologies, Korea University, Korea (South); Department Electronics and Information Engineering, Korea University, Korea (South)

An Effective Denial of Service Detection Method using Kernel Based Data [#7] *9*

Manhyun Chung, Jaeik Cho and Jongsub Moon

Center for Information Security Technologies, Korea University, Korea (South); Department Electronics and Information Engineering, Korea University, Korea (South)

A Case Study: Using Architectural Features to Improve Sophisticated Denial-of-Service Attack Detections [#22] *13*

Ran Tao, Li Yang, Lu Peng, Bin Li and Alma Cemerlic

Louisiana State University, United States; University of Tennessee at Chattanooga, United States

Cognitive Security Management with Reputation based Cooperation Schemes in Heterogeneous Networks [#37] *19*

Minsoo Lee, Xiaohui Ye, Samuel Johnson, Dan Marconett, S. K. Chaitanya Vadrevu, Rao Vemuri and S. J. Ben Yoo

University of California, Davis, United States

Session CICS-2: Keynote Lecture 1
Wednesday, April 1, 11:00AM-11:50AM, Room: Belmont, Chair: Dipankar Dasgupta, University of Memphis, USA

Internet Security Threat Landscape: Scaling to Meet the Threat

Robert Stratton

Symantec Research Labs, United States

Session CICS-3: Malicious Code Detections
Wednesday, April 1, 11:50AM-1:00PM, Room: Belmont, Chair: Justin Zhan, Carnegie Mellon University, USA, and Dipankar Dasgupta, University of Memphis, USA

Study of Fuzzy Clustering Methods for Malicious Codes Using Native API Call Frequency [#4] *24*

Ochul Kwon, Seongjae Bae, Jaeik Cho and Jongsub Moon

Center for Information Security Technologies, Korea University, Korea (South); Department Electronics and Information Engineering, Korea Univiersity, Korea (South)

Visual Similarity-based Phishing Detection without Victim Site Information [#16] *30*

Masanoei Hara, Akira Yamada and Yutaka Miyake

KDDI Research and Development Laboratories Inc., Japan; KDDI Research and Development Laboratories Inc., Kiribati

Characterizing Comment Spam in the Blogosphere through Content Analysis [#19] *37*

Archana Bhattarai, Vasile Rus and Dipankar Dasgupta

The University of Memphis, United States

Session CICS-4: File, Data and Process Security and Analysis

Wednesday, April 1, 2:00PM-4:00PM, Room: Belmont, Chair: Frederick Sheldon, Oak Ridge National Laboratory, USA, and Robert Abercrombie, Oak Ridge National Laboratory, USA

Enhancing File Data Security in Linux Operating System by Integrating Secure File System [#13] *45*

Rajesh Kumar Pal and Indranil Sengupta

Indian Institute of Technology, Delhi, India; Indian Institute of Technology, Kharagpur, India

Email Worm Detection by Wavelet Analysis of DNS Query Streams [#21] *53*

Nikolaos Chatzis, Radu Popescu-Zeletin and Nevil Brownlee

Fraunhofer Institute Fokus, Germany; The University of Auckland, New Zealand

Visualization of Security Events Using an Efficient Correlation Technique [#24] *61*

Qishi Wu, Ferebee Denise, Lin Yunyue and Dasgupta Dipankar

The University of Memphis, United States

Managing Complex IT Security Processes with Value Based Measures [#33] *69*

Robert Abercrombie, Frederick Sheldon and Ali Mili

Oak Ridge National Laboratory, United States; New Jersey Institute of Technology, United States

JigDFS: A Secure Distributed File System [#36] *76*

Jiang Bian and Remzi Seker

Computer Science, University of Arkansas at Little Rock, United States

Session CICS-5: Intrusion Detection Systems
Wednesday, April 1, 4:30PM-6:30PM, Room: Belmont, Chair: Remzi Seker, University of Arkansas at Little Rock, USA

Detection of Intrusive Activity in Databases by Combining Multiple Evidences and Belief Update [#6] 83
Suvasini Panigrahi, Shamik Sural and Arun Kumar Majumdar
School of Information Technology, IIT Kharagpur, India; Dept. of Computer Science and Engineering, IIT Kharagpur, India

Using Qualia and Multi-Layered Relationships in Malware Detection [#25] 91
Bobby Birrer, Richard Raines, Rusty Baldwin, Mark Oxley and Steven Rogers
Air Force Institute of Technology, United States; Air Force Research Laboratory, United States

An Unsupervised Method For Intrusion Detection Using Spectral Clustering [#28] 99
Siddharth Gujral, Estefan Ortiz and Vassilis Syrmos
University Of Hawaii at Manoa, United States

Environmental Awareness Intrusion Detection and Prevention Systems toward reducing False Positives and False Negatives [#32] 107
Sourour Meharouech, Adel Bouhoula and Tarek Abbes
Higher School of Communication, Tunisia

Session CICS-6: Keynote Lecture 2
Thursday, April 2, 8:30AM-9:30AM, Room: Belmont, Chair: Dipankar Dasgupta, University of Memphis, USA

TBA
Sean McGurk
Department of Homeland Security, United States

Session CICS-7: Keynote Lecture 3
Thursday, April 2, 9:30AM-10:30AM, Room: Belmont, Chair: Dipankar Dasgupta, University of Memphis, USA

Privacy-Preserving Collaborative Data Mining
Justin Zhan
Carnegie Mellon University, United States

Session CICS-8: Bio-Inspired Approaches
Thursday, April 2, 11:00AM-1:00PM, Room: Belmont, Chair: S. J. Ben Yoo, University of California - Davis, USA, and Dipankar Dasgupta, University of Memphis, USA

Genetic Algorithm Cryptanalysis of a Substitution Permutation Network [#2] 115
Joseph Brown, Sheridan Houghten and Beatrice Ombuki-Berman
Brock University, Canada

A Self-Organizing Map and its Modeling for Discovering Malignant Network Traffic [#8] 122
Chet Langin, Hongbo Zhou, Shahram Rahimi, Mehdi Zargham, Mohammad Sayeh and Bidyut Gupta
Southern Illinois University Carbondale, United States

User Identification Using GUI Manipulation Patterns and Artificial Neural Networks [#26] 130
Eric Imsand, Deon Garrett and John A. Hamilton
University of Memphis, United States; Auburn University, United States

Generating Mimicry Attacks using Genetic Programming: A Benchmarking Study [#29] 136
Gunes Kayacik, Nur Zincir-Heywood, Malcolm Heywood and Stefan Burschka
Dalhousie University, Canada; Swisscom Innovations, Switzerland

Network Security Using Self Organized Agent Swarms [#31] 144
Eric Holloway, Gary Lamont and Gilbert Peterson
AFIT, United States

Session CICS-9: Miscellaneous topics
Thursday, April 2, 2:00PM-4:00PM, Room: Belmont, Chair: Justin Zhan, Carnegie Mellon University, USA, and Li Yang, University of Tennessee at Chattanooga, USA

Finding the State Sequence Maximizing P(O,I * *) on Distributed HMMs with Privacy [#1] 152
Sahin Renckes, Huseyin Polat and Yusuf Oysal
Anadolu University, Turkey

A Compiler Classification Framework for Use in Reverse Engineering [#3] 159
Stephen Torri, Winard Britt and John Hamilton
Auburn University, United States

Generalization of Signatures for SSH Encrypted Traffic Identification [#20] 167
Riyad Alshammari and A. Nur Zincir-Heywood
Dalhousie University, Canada

Discovering Latent Topics from Dark Websites [#27] 175
Li Yang, Feiqiong Liu, Joseph Kizza and Raimund Ege
University of Tennessee at Chattanooga, United States; Northern Illinois University, United States

AUTHOR INDEX