2011 IEEE Symposium on Computational Intelligence in Cyber Security

(CICS 2011)

Paris, France
11 – 15 April 2011

IEEE Catalog Number: CFP11CIY-PRT
ISBN: 978-1-4244-9905-2

TABLE OF CONTENTS

INTRUSION/ANAMOLY DETECTION

Autonomous Rule Creation for Intrusion Detection 1
T. Vollmer, J. Alves-Foss, M. Manic

Automatic Construction of Anomaly Detectors from Graphical Models 9
E. Ferragut, D. Darmon, C. Shue, S. Kelley

An Effective Network-based Intrusion Detection Using Conserved Self Pattern Recognition Algorithm Augmented with Near-deterministic Detector Generation 17
S. Yu, D. Dasgupta

POSTER SESSION

Modeling Cyber Knowledge Uncertainty 25
D. Lee, S. Hamilton, W. Hamilton

A Hybrid of the Prefix Algorithm and the q-hidden Algorithm for Generating Single Negative Databases 31
R. Liu, W. Luo, X. Wang

Security Fusion Based On State Machine Compositions 39
O. Ibrahim, S. Nair

Discrimination Prevention in Data Mining for Intrusion and Crime Detection 47
S. Hajian, J. Domingo-Ferrer, A. Martinez-Balleste

Phishing Detection Using Stochistic Learning-Based Weak Estimators 55
J. Zhan, L. Thomas

MISSION ASSURANCE

Modeling Cyber Conflicts Using an Extended Petri Net Formalism 60
A. Zakrzewska, E. Ferragut

Addressing the Need for Independence in the CSE Model 68
R. Abercrombie, E. Ferragut, F. Sheldon, M. Grimaila

A Scalable Architecture for Improving the Timeliness and Relevance of Cyber Incident Notifications 76
J. Miller, R. Mills, M. Grimaila, M. Haas

Design Considerations for a Case-Based Reasoning Engine for Scenario-Based Cyber Incident Notification 84
S. Woskov, M. Grimaila, R. Mills, M. Haas

An Approach to the Automated Determination of Host Information Value 92
J. Beaver, R. Patton, T. Potok

Multi Agent Systems on Military Networks 100
D. Hancock, G. Lamont

SOCIAL MEDIA AND DATA SECURITY

Hierarchical Traceability Of Multimedia Documents 108
A. Hamida, M. Koubaa, C. Amar, H. Nicolas

A Host Based DES Approach for Detecting ARP Spoofing 114
F. Barbhuiya, S. Biswas, N. Hubballi, S. Nandi

Profiling File Repository Access Patterns for Identifying Data Exfiltration Activities 122
Y. Hu, C. Frank, J. Walden, E. Crawford, D. Kasturiratna

Game Theory-based Defense Mechanisms against DDoS Attacks on TCP/TCP-friendly Flows 129
H. Bedi, S. Roy, S. Shiva

Trust Optimization in Task-Oriented Social Networks 137
J. Zhan, X. Fang, P. Killion

Wireless Security Situation Awareness with Attack Identification Decision Support 144
P. Harmer, R. Thomas, B. Christel, R. Martin, C. Watson

Location Privacy Protection on Social Networks 152
J. Zhan, X. Fang, N. Bandaru
Security Visualization: Cyber Security Storm Map and Event Correlation 156
D. Ferebee, D. Dasgupta, M. Schmidt, Q. Wu
Large In-Memory Cyber-Physical Security-Related Analytics via Scalable Coherent Shared Memory Architectures 164
J. Williams, S. Herrero, C. Leonardi, S. Chan, A. Sanchez, Z. Aung
Biodiversity: A Security Approach for Ad Hoc Networks 173
J. Jackson, S. Creese, M. Leeson

TOPICS ON CYBER SECURITY

Exploring the State Space of an Application Protocol: A Case Study of SMTP 181
P. Laroche, A. Zincir-Heywood, M. Heywood
Genetic Optimization and Hierarchical Clustering Applied to Encrypted Traffic Identification 189
C. Bacquet, A. Zincir-Heywood, M. Heywood
Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor 197
O. Linda, M. Manic, T. Vollmer, J. Wright
A Systems Engineering Approach For Crown Jewels Estimation And Mission Assurance Decision Making 205
S. Musman, M. Tanner, A. Temin, E. Elsaesser, L. Loren
Intelligence, Not Integration: Distributed Regret Minimization for IDS Control 212
M. Rehak, J. Stiborek, M. Grill
Author Index