

Preface

In terms of network science and cybersecurity, the challenge is the ability to perceive, discover, and prevent malicious actions or events within the network. It is clear that the amount of information traffic data types has been continuously growing which makes the job of a security analyst increasingly difficult and complex. Therefore, it is the goal of this book to offer basic research solutions into promising emerging technologies that will offer and enable enhanced cognitive and high performance capabilities to the human analyst charged with monitoring and securing the network. The work contained herein describes the following research ideas.

[Towards Fundamental Science of Cyber Security](#) provides a framework describing commonly used terms like “Science of Cyber” or “Cyber Science” which have been appearing in the literature with growing frequency, and influential organizations initiated research initiatives toward developing such a science even though it is not clearly defined. The chapter offers a simple formalism of the key objects within cyber science and systematically derives a classification of primary problem classes within the science.

[Bridging the Semantic Gap—Human Factors in Anomaly-Based Intrusion Detection Systems](#) examines the “semantic gap” with reference to several common building blocks for anomaly-based intrusion detection systems. Also, the chapter describes tree-based structures for rule construction similar to those of modern results in ensemble learning, and suggests how such constructions could be used to generate anomaly-based intrusion detection systems that retain acceptable performance while producing output that is more actionable for human analysts.

[Recognizing Unexplained Behavior in Network Traffic](#) presents a framework for evaluating the probability that a sequence of events is not explained by a given set of models. The authors leverage important properties of this framework to estimate such probabilities efficiently, and design fast algorithms for identifying sequences of events that are unexplained with a probability above a given threshold.

[Applying Cognitive Memory to CyberSecurity](#) describes a physical implementation in hardware of neural network algorithms for near- or real-time data mining, sorting, clustering, and segmenting of data to detect and predict criminal

behavior using Cognimem's CM1 K cognitive memory as a practical and commercially available example. The authors describe how a vector of various attributes can be constructed, compared, and flagged within predefined limits.

Understanding Cyber Warfare discusses the nature of risks and vulnerabilities and mitigating approaches associated with the digital revolution and the emergence of the World Wide Web. The discussion geared mainly to articulating suggestions for further research rather than detailing a particular method.

Design of Neuromorphic Architectures with Memristors presents the design criteria and challenges to realize Neuromorphic computing architectures using emerging memristor technology. In particular, the authors describe memristor models, synapse circuits, fundamental processing units (neural logic blocks), and hybrid CMOS/memristor neural network (CMHNN) topologies using supervised learning with various benchmarks.

Nanoelectronics and Hardware Security focuses on the utilization of nanoelectronic hardware for improved hardware security in emerging nanoelectronic and hybrid CMOS-nanoelectronic processors. Specifically, features such as variability and low power dissipation can be harnessed for side-channel attack mitigation, improved encryption/decryption, and anti-tamper design. Furthermore, the novel behavior of nanoelectronic devices can be harnessed for novel computer architectures that are naturally immune to many conventional cyber attacks. For example, chaos computing utilizes chaotic oscillators in the hardware implementation of a computing system such that operations are inherently chaotic and thus difficult to decipher.

User Classification and Authentication for Mobile Device Based on Gesture Recognition describes a novel user classification and authentication scheme for mobile devices based on continuous gesture recognition. The user's input patterns are collected by the integrated sensors on an Android smartphone. A learning algorithm is developed to uniquely recognize a user during their normal interaction with the device while accommodating hardware and biometric features that are constantly changing. Experimental results demonstrate a great possibility for the gesture-based security scheme to reach sufficient detection accuracy with an undetectable impact on user experience.

Hardware-Based Computational Intelligence for Size, Weight, and Power Constrained Environments examines the pressures pushing the development of unconventional computing designs for size, weight, and power constrained environments and briefly reviews some of the trends that are influencing the development of solid-state neuromorphic systems. The authors also provide high level examples of selected approaches to hardware design and fabrication.

Machine Learning Applied to Cyber Operations investigates machine learning techniques that are currently being researched and are under investigation within the Air Force Research Laboratory. The purpose of the chapter is primarily to educate the reader on some machine learning methods that may prove helpful in cyber operations.

Detecting Kernel Control-flow Modifying Rootkits proposes a Virtual Machine Monitor (VMM)-based framework to detect control-flow modifying kernel rootkits

in a guest Virtual Machine (VM) by checking the number of certain hardware events that occur during the execution of a system call. Our technique leverages the Hardware Performance Counters (HPCs) to securely and efficiently count the monitored hardware events. By using HPCs, the checking cost is significantly reduced and the temper-resistance is enhanced.

Formation of Artificial and Natural Intelligence in Big Data Environment discusses Holographic Universe representation of the physical world and its possible corroboration. The author presents a model that captures the cardinal operational feature of employing unconsciousness for Big Data and suggests that models of the brain without certain emergent unconsciousness are inadequate for handling the Big Data situation. The suggested “Big Data” computational model utilizes all the available information in a shrewd manner by manipulating explicitly a small portion of data on top of an implicit context of all other data.

Alert Data Aggregation and Transmission Prioritization over Mobile Networks presents a novel real-time alert aggregation technique and a corresponding dynamic probabilistic model for mobile networks. This model-driven technique collaboratively aggregates alerts in real-time, based on alert correlations, bandwidth allocation, and an optional feedback mechanism. The idea behind the technique is to adaptively manage alert aggregation and transmission for a given bandwidth allocation. This adaptive management allows the prioritization and transmission of aggregated alerts in accordance with their importance.

Semantic Features from Web-traffic Streams describes a method to convert web-traffic textual streams into a set of documents in a corpus to allow use of established linguistic tools for the study of semantics, topic evolution, and token-combination signatures. A novel web-document corpus is also described which represents semantic features from each batch for subsequent analysis. This representation thus allows association of the request string tokens with the resulting content, for consumption by document classification and comparison algorithms.

Concurrent Learning Algorithm and the Importance Map presents machine learning and visualization algorithms developed by the U.S. National Security Agency’s Center for Exceptional Computing. The chapter focuses on a cognitive approach and introduces the algorithms developed to make the approach more attractive. The Concurrent Learning Algorithm (CLA) is a biologically inspired algorithm, and requires a brief introduction to neuroscience. Finally, the Importance Map (IMAP) algorithm will be introduced and examples given to clearly illustrate its benefits.

Hardware Accelerated Mining of Domain Knowledge introduces cognitive domain ontologies (CDOs) and examines how they can be transformed into constraint networks for processing on high-performance computer platforms. The constraint networks were solved using a parallelized generate and test exhaustive depth first search algorithm. Two compute platforms for acceleration are examined: Intel Xeon multicore processors, and NVIDIA graphics processors (GPGPUs). The scaling of the algorithm on a high-performance GPGPU cluster achieved estimated speed-ups of over 1,000 times.

Memristors and the Future of Cyber Security Hardware covers three approaches to emulate a memristor-based computer using artificial neural networks and describes how a memristor computer could be used to solve Cyber security problems. The memristor emulation neural network approach was divided into three basic deployment methods: (1) deployment of neural networks on the traditional Von Neumann CPU architecture, (2) software-based algorithms deployed on the Von Neumann architecture utilizing a Graphics Processing Units (GPUs), and (3) a hardware architecture deployed onto a field-programmable gate array.

This book is suitable for engineers, technicians, and researchers in the fields of cyber research, information security and systems engineering, etc. It can also be used as a textbook for senior undergraduate and graduate students. Postgraduate students will also find this a useful sourcebook since it shows the direction of current research. We have been fortunate in attracting outstanding class researchers as contributors and wish to offer our thanks for their support in this project.

Dr. Robinson E. Pino works with ICF International and has expertise within technology development, program management, government, industry, and academia. He advances state-of-the-art cybersecurity solutions by applying autonomous concepts from computational intelligence and neuromorphic computing. Previously, Dr. Pino was a senior electronics engineer at the U.S. Air Force Research Laboratory (AFRL) where he was a program manager and principle scientist for the computational intelligence and neuromorphic computing research efforts. He also worked at IBM as an advisory scientist/engineer development enabling advanced CMOS technologies and as a business analyst within IBM's photomask business unit. Dr. Pino also served as an adjunct professor at the University of Vermont where he taught electrical engineering courses.

Dr. Pino has a B.E. in Electrical Engineering from the City University of New York and an M.Sc. and a Ph.D. in Electrical Engineering from the Rensselaer Polytechnic Institute. He is the recipient of numerous awards and professional distinctions; has published more than 40 technical papers, including three books; and holds six patents, three pending.

This work is dedicated to Dr. Pino's loving and supporting wife without whom this work would not be possible.

ICF International, Fairfax, USA

Dr. Robinson E. Pino



<http://www.springer.com/978-1-4614-7596-5>

Network Science and Cybersecurity

Pino, R.E. (Ed.)

2014, X, 285 p., Hardcover

ISBN: 978-1-4614-7596-5