baratz | ODA

Cybersecurity and High-Performance Computing Environments : Integrated Innovations, Practices, and Applications

Li, Kuan-Ching.
Providence University Taiwan
Sukhija, Nitin
Bautista, Elizabeth
Gaudiot, Jean-Luc

Electronic books

Monografía

In this fast-paced global economy, academia and industry must innovate to evolve and succeed. Today's researchers and industry experts are seeking transformative technologies to meet the challenges of tomorrow. The cutting-edge technological advances in cybersecurity solutions aids in enabling the security of complex heterogeneous high-performance computing environments. On the other hand, high-performance computing power facilitates powerful and intelligent innovative models for reducing time to response to identify and resolve a multitude of potential new emerging cyber-attacks. Cybersecurity and High-Performance Computing Environments provides a collection of the current and emergent research innovations, practices, and applications focusing on the interdependence of cybersecurity and high-performance computing domains for discovering and resolving new emerging cyber-threats. Key Features: Represents a substantial research contribution to state-of-the-art solutions for addressing the threats to Confidentiality, Integrity, and Availability (CIA Triad) in high-performance computing (HPC) environments. Covers the groundbreaking and emergent solutions that utilize the power of the HPC environments to study and understand the emergent multifaceted anomalous and malicious characteristics. The content will help university students, researchers, and professionals understand how high-performance computing research fits broader cybersecurity objectives and vice versa

https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMzA3ODQ3OTc

Título: Cybersecurity and High-Performance Computing Environments Integrated Innovations, Practices, and Applications

Edición: 1st ed

Editorial: [Place of publication not identified] Chapman and Hall/CRC 2022

Descripción física: 1 online resource (395 pages)

Contenido: Cover -- Half Title -- Title Page -- Copyright Page -- Table of Contents -- PREFACE -- EDITORS -- CONTRIBUTORS -- CHAPTER 1 Cybersecurity and High-Performance Computing Ecosystems: Opportunities and Challenges -- 1.1 Introduction -- 1.2 The Vital Importance of Securing High-Performance Computing (HPC) Ecosystems -- 1.3 Security for Supercomputing Infrastructure -- 1.3.1 Software Security -- 1.3.2 Hardware Security -- 1.4 Applications Security -- 1.5 Data Security in HPC Ecosystems -- 1.6 User-Specific Cybersecurity -- 1.6.1 Policies -- 1.7 Discussion and Summary -- References -- CHAPTER 2 Approaches to Working with Large-Scale Graphs for Cybersecurity Applications -- 2.1 Introduction -- 2.2 Generation -- 2.2.1 Generation Introduction -- 2.2.2 Algorithm Walk-Throughs -- 2.2.2.1 Introduction -- 2.2.2.2 Attack Graphs -- 2.2.2.3 Attack Dependency Graphs -- 2.2.2.4 Combination of Attack Graphs and Attack Dependency Graphs -- 2.2.2.5 Compliance Graphs -- 2.2.3 Parallel Generation Algorithms -- 2.2.4 Additional Architectural and Hardware Techniques -- 2.2.4.1 Prefetching -- 2.2.4.2 Accelerators -- 2.2.4.3 Better Data Structures -- 2.2.4.4 Useful Libraries -- 2.2.5 Deploying to High-Performance Computing Clusters -- 2.2.5.1 Base Approach: General Parallelized Programming -- 2.2.5.2 Programming Model Optimizations -- 2.3 Analysis -- 2.3.1 Introduction -- 2.3.2 Markov Process Model -- 2.3.3 Shortest Path -- 2.3.3.1 Dijkstra's Algorithm -- 2.3.3.2 Bellman-Ford Algorithm -- 2.3.3.3 Parallel APSP -- 2.3.4 Minimization -- 2.3.5 Criticality -- 2.3.6 Semi-Metricity -- 2.4 Conclusions and Future Work -- References -- CHAPTER 3 OMNI at the Edge -- 3.1 Introduction -- 3.2 Background -- 3.3 OMNI Architecture and Technologies -- 3.3.1 OMNI k3s Architecture -- 3.3.2 Use of Edge Computing in OMNI -- 3.3.3 Securing Small Devices at the Edge 3.3.4 Function as a Service at the Edge -- 3.3.5 Analysis at the Edge for Diagnostic and Troubleshooting Issues -- 3.4 Case Study of Benefits of OMNI Data to NERSC Data Center -- 3.4.1 2M Mechanical Substation Cost Savings -- 3.4.2 Perlmutter Power Upgrade from 12.5 to 25.0 MW -- 3.4.3 Edge Service to Mitigate California's Public Safety Power Shutdown (PSPS) -- 3.5 Ongoing and Future Work -- References -- CHAPTER 4 Optimized Voronoi-Based Algorithms for Parallel Shortest Vector Computation -- 4.1 Introduction -- 4.2 SVP-Solvers Based on Voronoi Cells -- 4.2.1 Voronoi Cell-Based Algorithm by Micciancio et al. -- 4.2.2 Relevant Vectors by Agrell et al. -- 4.3 Experimental Setup -- 4.4 Algorithm Analysis -- 4.4.1 Correlation between the Norm of Target Vectors and Solution Vectors -- 4.4.2 Percentage of Target Vectors That Generate the Shortest Vector -- 4.5 Algorithmic Optimizations -- 4.5.1 Pruned Decoding -- 4.5.1.1 Simple pruning -- 4.5.1.2 Gaussian Pruning -- 4.5.1.3 Combined Pruning -- 4.5.2 Increasing Norm Sort -- 4.6 Parallel Implementations for CPUs and GPUs -- 4.6.1 CPU -- 4.6.1.1 Original Version (No Pruning and No Pre-Sorting) -- 4.6.1.2 Pruned Version without Sorting -- 4.6.1.3 Pruned Version with Sorting -- 4.6.2 GPU -- 4.7 Discussion -- 4.8 Conclusions -- 4.8.1 Open Problems -- Acknowledgments -- Notes -- References -- CHAPTER 5 Attribute-Based Secure Keyword Search for Cloud Computing -- 5.1 Introduction -- 5.2 Key Techniques in ABKS -- 5.2.1 Attribute-Based Encryption -- 5.2.1.1 Preliminaries in ABE -- 5.2.1.2 A CP-ABE Construction -- 5.2.2 Searchable Encryption -- 5.2.2.1 SE in the Private-Key Setting -- 5.2.2.2 SE in the Public-Key Setting -- 5.3 ABKS Construction -- 5.3.1 System Model and Threat Model -- 5.3.1.1 System Model -- 5.3.1.2 Threat Model -- 5.3.2 Basic Algorithm -- 5.3.2.1 Algorithm Definition 5.3.2.2 Algorithm Implementation -- 5.3.3 Search Privilege Revocation -- 5.3.3.1 Coarse-Grained Revocation -- 5.3.3.2 Fine-Grained Revocation -- 5.4 Experimental Result Analysis -- 5.5 Conclusions and Future Directions -- References -- CHAPTER 6 Understanding Cybersecurity Risk in FMI Using HPC -- 6.1 Introduction -- 6.2 What Is Financial Market Infrastructure (FMI)? -- 6.2.1 Payment Systems -- 6.2.2 Central Security Depositories -- 6.2.3 Security Settlement Systems -- 6.2.4 Central Counterparties -- 6.2.5 Trade Repositories -- 6.3 What Is High-Performance Computing? -- 6.4 How HPC Could Transform the Financial Industry -- 6.5 HPC in FMIs -- 6.6 Current Works on Cybersecurity Issues Related to HPC in FMIs -- 6.7 Financial Risks in FMIs -- 6.8 Common Security Objectives -- 6.9 Cybersecurity Issues and Financial Risks in FMIs -- 6.10 Cybersecurity Risks in FMIs -- 6.10.1 Cybersecurity Risks -- 6.10.2 Risk Assessment -- 6.10.3 Risk Analysis -- 6.10.4 Risk Monitoring, Reporting, and Mitigation -- 6.11 Conclusions -- References -- CHAPTER 7 Live Migration in HPC -- 7.1 Introduction -- 7.1.1 Introduction to Live Migration -- 7.1.1.1 Needs -- 7.1.1.2 Applications -- 7.1.1.3 Efficiency -- 7.1.1.4 Security -- 7.1.2 Introduction to Cloud Computing -- 7.2 Live Migration in VM -- 7.2.1 Live VM Migration Techniques in Cloud -- 7.2.1.1 Post-Copy Approach -- 7.2.1.2 Pre-Copy Approach -- 7.2.2 Research Challenges in VM Migration -- 7.2.3 Security in Live VM Migration -- 7.3 Live Container Migration -- 7.3.1 Migration -- 7.3.1.1 Memory Migration -- 7.3.1.2 Network Migration -- 7.3.2 Type of Migration to Manage Cache Transfers -- 7.3.2.1 Suspend /Resume Migration -- 7.3.2.2 Record-Replay Migration -- 7.3.3 Case Study -- 7.3.3.1 Checkpointing and Restoring in CRIU -- 7.3.3.2 Checkpointing and Restoring in OpenVZ -- 7.3.4 Performance 7.3.5 Comparing VMs vs.

Containers via High-Availability/Fault Tolerance (HA/FT) Solutions -- 7.3.5.1 HA in Hypervisor-Based Platforms -- 7.3.5.2 HA in Container-Based Platforms -- 7.3.5.3 Clustering Efforts for Containers -- 7.4 Attacks on Live Migration -- 7.4.1 Improper Access Control Policies -- 7.4.2 Unprotected Transmission Channel -- 7.4.3 Loopholes in Migration Module -- 7.5 Approaches -- 7.5.1 Isolating the Migration Traffic -- 7.5.2 Network Security Engine-Hypervisor (NSE-H) -- 7.6 Summary -- References -- CHAPTER 8 Security-Aware Real-Time Transmission for Automotive CAN-FD Networks -- 8.1 Introduction -- 8.1.1 Background and Motivation -- 8.1.2 Contributions and Outline -- 8.2 Automotive CAN-FD Networks Preliminaries -- 8.2.1 Differences between CAN-FD and CAN -- 8.2.2 Security Vulnerabilities in CAN-FD -- 8.2.3 Automotive Cyber-Attack Model -- 8.3 Automotive CAN-FD Security-Aware Real-Time Transmission Methods -- 8.3.1 Automotive CAN-FD Security-Aware Real-Time Transmission Constraints -- 8.3.2 Confidentiality-Aware Real-Time Transmission -- 8.3.2.1 Symmetric-Key Cryptography -- 8.3.2.2 Asymmetric-Key Cryptography -- 8.3.2.3 Key Distribution -- 8.3.2.4 Hardware Security Module -- 8.3.3 Integrity-Aware Real-Time Transmission -- 8.3.3.1 Hash-Based Message Authentication Code -- 8.3.3.2 Cipher-Based Message Authentication Codes -- 8.3.3.3 Digital Signature -- 8.3.4 Availability-Aware Real-Time Transmission -- 8.3.4.1 Authentication and Authorization -- 8.3.4.2 Obfuscating Priority Assignment -- 8.3.4.3 Intrusion Detection -- 8.4 Future Trends -- 8.5 Conclusions -- References -- CHAPTER 9 OntoEnricher: A Deep Learning Approach for Ontology Enrichment from Unstructured Text -- 9.1 Introduction -- 9.2 Related Work -- 9.3 Ontology Enrichment Approach -- 9.3.1 Stage 1: Creation of Dataset -- 9.3.2 Stage 2: Creation of Corpus 9.3.3 Stage 3: Training OntoEnricher -- 9.3.4 Stage 4: Testing OntoEnricher -- 9.3.5 Example -- 9.4 Experimental Settings and Results -- 9.5 Conclusion and Future Work -- Notes -- References -- CHAPTER 10 Intelligent Connected Vehicles -- 10.1 Introduction -- 10.1.1 Intelligent Connected Vehicle (ICV) -- 10.1.2 Contributions and Chapter Organization -- 10.2 Cybersecurity Analysis of In-Vehicle Network -- 10.2.1 In-Vehicle Networks of ICV -- 10.2.2 Vulnerabilities and Cybersecurity Requirements -- 10.2.3 Attack Model and Vulnerabilities from External Interface Layer -- 10.2.4 Attack Model and Vulnerabilities from Network Layer -- 10.2.5 Attack Model and Vulnerabilities from Application Layer -- 10.3 Overview of Intelligent Connected Vehicle Cybersecurity Enhancement Countermeasures -- 10.3.1 Hardware Security Module -- 10.3.2 Message Authentication -- 10.3.3 Intrusion Detection System (IDS) -- 10.4 State-of-the-Art In-Vehicle Network Intrusion Detection Approaches -- 10.4.1 Feature-Based Observation Approaches -- 10.4.2 Statistical Analysis-Based Approaches -- 10.4.3 Artificial Intelligence-Based Approaches -- 10.5 Summary and Future Research -- References -- CHAPTER 11 Toward Robust Deep Learning Systems against Deepfake for Digital Forensics -- 11.1 Introduction -- 11.2 Background -- 11.3 Deepfake Forensics -- 11.3.1 Limitations in Digital Forensic Processes -- 11.3.2 Limitations in Digital Forensic Methods -- 11.3.2.1 Technical Response and Future -- 11.4 Related Work -- 11.4.1 Detecting in Pixel Level -- 11.4.2 Subtle Difference Collecting -- 11.4.3 Modifying the Architecture of CNN -- 11.4.4 Obtaining Fingerprint of GANs -- 11.4.5 Deepfake Video Forensic Methods -- 11.4.6 Datasets -- 11.4.7 Software for Deepfake Forensics -- 11.4.8 Challenges -- 11.5 Approach to Deepfake Forensics -- 11.5.1 Application Overview -- 11.5.2 Application Design 11.5.3 Model Training and Application Deployment

ISBN: 1-000-55366-3 1-003-15579-0

Materia: Computer security COMPUTERS / General COMPUTERS / Computer Graphics / Game Programming & Design COMPUTERS / Computer Science

Autores: Li, Kuan-Ching. Providence University Taiwan Sukhija, Nitin Bautista, Elizabeth Gaudiot, Jean-Luc

Enlace a formato físico adicional: 0-367-71150-8

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es