MIHAILO ISAKOV

PERSONAL INFORMATION

email	mihailo@tamu.edu
website	https://ascslab.org/members/mihailo/index.html
phone	+1 541 780 3005

RESEARCH INTERESTS

Intersection of computer architecture, machine learning, high performance computing, and security with a particular emphasis on: hardware and ML algorithm co-design, HPC I/O throughput modelling, secure execution of machine learning models, hardware acceleration of deep neural network (DNN) training, edge-deployed, low power, and low latency DNN training.

EDUCATION

Ph.D., Electrical and Computer Engineering

2020–2022 **Texas A&M University, College Station, TX**
Advisor: Prof. Michel A. Kinsy

Ph.D., Electrical and Computer Engineering

2016–2020 **Boston University, Boston, MA**
Advisor: Prof. Michel A. Kinsy
Laboratory transferred to Texas A&M University in September 2020.

Masters in Software Engineering

2015–2016 **University of Novi Sad, Novi Sad, Serbia**
Transferred in second year to the Boston University's Doctoral Program.

Bachelor in Electrical Engineering

2011–2015 *Software Engineering Specialization*
University of Novi Sad, Novi Sad, Serbia
Undergraduate Thesis Title: Inertial Motion Capture System Body Pose Reconstruction using Machine Learning.

WORK EXPERIENCE

Freelance Researcher

2015–2016 **Machine learning and data science**
Worked as a freelance researcher for several machine learning startups.

Teaching Assistant

2015–2016 **University of Novi Sad, Novi Sad, Serbia**
Prepared and taught labs for the (1) artificial intelligence and (2) soft computing classes.

Research intern

Jul–Sep 2014 **Xsens Technologies B.V. Enschede, Netherlands**
Researched efficient implementations of a human pose reconstruction algorithm from a limited number of inertial motion capture sensors worn on the body.

Co-founder / CTO

2013–2014 **Citrus Tech Design**
Co-founded startup building smart skateboards, longboards and snowboards.
Product video: LightBoard

CONFERENCE PUBLICATIONS

1. G. Dessouky, **M. Isakov**, M. Kinsy, P. Mahmoody, M. Mark, A. Sadeghi, E. Stapf, S. Zeitouni, "Distributed Memory Guard: Enabling Secure Enclave Computing in NoC-based Architectures" in 2021 58th ACM/ESDA/IEEE Design Automation Conference (DAC).
2. V. Gadepally, **M. Isakov**, R. Agrawal, J. Kepner, K. Gettings and M. A. Kinsy, "Homomorphic Encryption Based Secure Sensor Data Processing," 2020 IEEE High Performance Extreme Computing Conference (HPEC), 2020, pp. 1-7.
3. **M. Isakov**, E. del Rosario, S. Madireddy, P. Balaprakash, P. Carns, R. B. Ross, M. A. Kinsy, "HPC I/O Throughput Bottleneck Analysis with Explainable Local Models," in 2020 SC20: International Conference for High Performance Computing, Networking, Storage and Analysis (SC), Atlanta, GA, US, 2020 pp. 1-13.
4. **M. Isakov**, E. del Rosario, S. Madireddy, P. Balaprakash, P. Carns, R. B. Ross, M. A. Kinsy, "Toward Generalizable Models of I/O Throughput," 2020 IEEE/ACM International Workshop on Runtime and Operating Systems for Supercomputers (ROSS), GA, USA, 2020, pp. 41-49.
5. E. del Rosario, M. Currier, **M. Isakov**, S. Madireddy, P. Balaprakash, P. Carns, R. B. Ross, M. A. Kinsy, "Gauge: An Interactive Data-Driven Visualization Tool for HPC Application I/O Performance Analysis," 2020 IEEE/ACM Fifth International Parallel Data Systems Workshop (PDSW), GA, USA, 2020, pp. 15-21.
6. V. Gadepally, **M. Isakov**, R. Agrawal, J. Kepner, K. Gettings and M. A. Kinsy, "Homomorphic Encryption Based Secure Sensor Data Processing," 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 2020, pp. 1-7.
7. **M. Isakov**, V. Gadepally, K. M. Gettings and M. A. Kinsy, "Survey of Attacks and Defenses on Edge-Deployed Neural Networks," IEEE High Performance Extreme Computing Conference (**HPEC**), Waltham, MA, USA, 2019, pp. 1-8. **Best Student Paper Nominee**.
8. **M. Isakov**, L. Bu, H. Cheng, and M. A. Kinsy: Preventing Neural Network Model Exfiltration in Machine Learning Hardware Accelerators. In the 2018 Asian Hardware Oriented Security and Trust Symposium (**AsianHOST**), 2018.
9. **M. Isakov** and M. A. Kinsy: NoSync: Particle Swarm Inspired Distributed DNN Training. In the 27th International Conference on Artificial Neural Networks (**ICANN**), 2018.
10. **M. Isakov**, A. Ehret and M. Kinsy, "ClosNets: Batchless DNN Training with On-Chip a Priori Sparse Neural Topologies," 28th International Conference on Field Programmable Logic and Applications (**FPL**), Dublin, 2018, pp. 55-554.
11. **M. Isakov**, A. Ehret and M. Kinsy: Chameleon: A Generalized Reconfigurable Open-Source Architecture for Deep Neural Network Training. In the 2018 IEEE High Performance Extreme Computing Conference (**HPEC**), 2018. **Best student paper nominee**.
12. A. Ehret, **M. Isakov** and M. A. Kinsy: Towards a Generalized Reconfigurable Agent Based Architecture: Stock Market Simulation Acceleration, International Conference on Reconfigurable Computing and FPGAs (**ReConFig**), 2018.
13. J. R. Doppa, R. G. Kim, **M. Isakov**, M. A. Kinsy, H. Kwon and T. Krishna: Adaptive Manycore Architectures for Big Data Computing. In the International Symposium on Networks-on-Chip (**NOCS**), October 2017.
14. H. Hosseinzadeh, **M. Isakov**, M. Darabi, A. Patooghy, and M. Kinsy: Janus: An uncertain cache architecture to cope with side channel attacks. In 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (**MWSCAS**) Aug 2017. **The Myril B. Reed Best Paper Award**.
15. E. Taheri, **M. Isakov**, A. Patooghy, and M. Kinsy: Advertiser Elevator: a Fault Tolerant Routing Algorithm for Partially Connected 3D Network-on-Chips. In 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (**MWSCAS**) Aug 2017.
16. M. Kinsy, S. Khadka, **M. Isakov** and A. Farrukh: Hermes: Secure Heterogeneous Multicore Architecture Design. In the IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), May 2017.
17. M. Kinsy, S. Khadka and **M. Isakov**: PreNoc: Neural Network based Predictive Routing for Network-on-Chip Architectures. In the 27th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), May 2017.

JOURNAL PUBLICATIONS

1. E. Taheri, **M. Isakov**, A. Patooghy, M. A. Kinsy: Addressing a New Class of Reliability Threats in 3-Dimensional Network-on-Chips. In the Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), 2019.
2. M. A. Kinsy, L. Bu, **M. Isakov** and M. Mark: Designing Secure Heterogeneous Multicore Systems from Untrusted Components. **Cryptography**, vol. 2, iss. 3, no. 12, 2018.
3. L. Bu, **M. Isakov** and M. A. Kinsy: RASSS: A Hijack-resistant Confidential Information Management Scheme for Distributed Systems. In the Institution of Engineering and Technology (**IET**), - Computers and Digital Techniques, 2018.
4. L. Bu, **M. Isakov**, and M. A. Kinsy: A Secure and Robust Scheme for Sharing Confidential Information in IoT Systems. In the Elsevier Journal for Ad Hoc Networks, (**Ad Hoc Networks**), 2018.

WORKSHOP PUBLICATIONS

1. **M. Isakov**, ”Secure RISC-V Architectures Design Space Exploration Using the BRISC-V Platform”, Workshop on Secure RISC-V Architecture Design (SECRISC-V) 2020, Boston, MA.
2. N. Boskov, **M. Isakov** and M. A. Kinsy: CodeTrolley: Hardware-Assisted Control Flow Obfuscation. Boston Area Architecture 2019 Workshop (BARC19)
3. **M. Isakov** and M. A. Kinsy: NeuroFabric: A Priori Sparsity for Training on the Edge. In the 2019 tinyML Summit (tinyML), 2019.
4. R. Agrawal, S. Bandara, A. Ehret, **M. Isakov**, M. Mark, and M. A. Kinsy: The BRISC-V Platform: A Practical Teaching Approach for Computer Architecture, In Workshop on Computer Architecture Education (WCAE), 2019.
5. **M. Isakov** and M. A. Kinsy: ClosNets: a Priori Sparse Topologies for Faster DNN Training, Boston Area Architecture 2018 Workshop (BARC18), 2018.
6. M. A. Kinsy, **M. Isakov**, A. Ehret and D. Kava: SAPA: Self-Aware Polymorphic Architecture, Boston Area Architecture 2018 Workshop (BARC18), 2018.

REPORTS

1. **M. Isakov**, M. Kinsy. ”NeuroFabric: Identifying Ideal Topologies for Training A Priori Sparse Networks”, Report v1.0, Dec. 2019.
2. N. Boskov, **M. Isakov**, M. Kinsy. ”Drndalo: Lightweight Control Flow Obfuscation Through Minimal Processor/Compiler Co-Design”, arXiv preprint arXiv:1912.01560, 2019.
3. P. Ren, M. Kinsy, M. Zhu, S. Khadka, **M. Isakov**, A. Ramrakhyani, T. Krishna, and N. Zheng. FASHION: Fault-Aware Self-Healing Intelligent On-chip Network. arXiv:1702.02313, 2017.

OUTREACH ACTIVITIES

1. Summer 2019 - Cybersecurity: Introduction to Hardware Security - University of the Virgin Islands Summer Program
2. Summer 2017 - Summer Challenge: Electrical Engineering - For high school students as part of the Boston University Summer Program.

May 22, 2021