General Portfolio of Dr. Taheri's Laboratory at Gannon University

In the following, the general portfolio of Dr. Shayan (Sean) Taheri's planned research laboratory in the Department of Electrical and Computer Engineering (ECE) at the Gannon University (GU) is presented:

1. About

Dr. Taheri's laboratory will be established to be an outstanding and unique multidisciplinary research center in the advancement of cybersecurity as a basis for long-term partnership and collaboration among academia, industry, government, and private sectors. The laboratory's mission will be to: (1) directly support research needs of partners in a cost-effective manner with efficient and colligated resources and maximized synergy; and (2) enhance the educational experience for a diverse set of top-quality graduate- and undergraduate-level researchers and students. Dr. Taheri's center will advance knowledge and technologies in this emerging field and ensure commercial relevance of the research with rapid and effective technology transfer and establishing spin-off companies. It will be one of the few centers in the country that will provide excellent expertise in all aspects of cybersecurity and assurance including hardware, artificial intelligence, network, mobile, big data, internet of things, applied cryptography, social sciences, law, and more.

- Diversity: The center employees will feel valued, appreciated, respected, and free. The fundamental value and dignity of all individuals will be honored and acknowledged regardless of their race, religion, sexual orientation, or any other perceived difference. All members will be committed to practicing inclusion; fostering diversity among students, faculty, and staff; and eliminating discrimination in all its forms.

- Faculty: Dr. Shayan (Sean) Taheri. His major research interests are Computer Hardware, Cybersecurity, Artificial Intelligence, and Data Science.

- Students: Graduate and undergraduate students.

2. Research

With the emergence of information technology and its critical and indispensable role in our daily lives and the increasing complexity of networked computing systems, the risk of cyber-attacks is larger today than ever before that makes modern systems vulnerable to various attacks against their resources, infrastructure, and operability. While the reasons for such attacks may be tied to complex sociological issues, the defense solutions to confront them should be continuously studied for all system layers, i.e., Material and Physics, Nanoelectronic Device, Nanoelectronic Device-Level Circuit, Register Transfer Level (RTL) and Gate-Level Circuit, Microarchitecture, Instruction Set Architecture (ISA), Operating System and Virtual Machine, Programming Language, Algorithm, and Application. While there are abundant works on security of traditional software elements in computing systems, the research efforts on the security of hardware components as well as the intelligent software elements are insufficient, so the scientific community still lacks adequate and reliable knowledge about their principles, existing and emerging threats, and countermeasures for making the systems secure and protected.

The complexity of the design, fabrication, and distribution of electronics has caused a shift throughout the industry toward a global business model, thereby creating new sources of system vulnerabilities. In such a model, untrusted entities participate either directly or indirectly in all phases in the life of an electronic device or integrated circuit (IC). Due to this globalization, hardware underlying information systems have become increasingly targets of various malicious and stealthy attacks. To ensure the security of our critical infrastructure, the use of trusted hardware is absolutely necessary. On the other side, several security issues have been raised in critical applications due to the deployment of Artificial Intelligence (AI) in real-world applications (e.g., driverless cars, biometric/speech recognition system, and healthcare system) thanks to its provision of superior performance in identification and cognitive tasks. Besides several offenses on "normal" AI systems, the methods from AI can be leveraged by adversaries to perform intelligent malicious activities, leading to detrimental social, physical, and economic impacts. As a result, it is extremely challenging and timely mission for academic, industrial, and governmental institutions to comprehensively study and analyze the security aspects of hardware components and intelligent software elements in computing systems. Motivated by the above matters, Dr. Taheri's laboratory will focus on all directions of "Hardware Security" and "Security Aspects of Artificial Intelligence", aiming to make the next generation of computing systems more trustworthy. A number of these directions are mentioned in the following:

- System-on-Chip (SoC) Security and Trust
- Positive and Negative Applications of Emerging Transistor and Memory Technologies in Hardware Security
- Biometrics and Security
- Verification of Intellectual Property (IP) Security and Trust
- Physical Inspection and Assurance of Electronics
- Internet-of-Things (IoT) Security
- Nano-Scale Security
- Security of Electronics and Non-Electronics Supply Chain
- Security of Cyber Physical Systems
- Post-Quantum and Applied Cryptography and Privacy
- Security of Cloud and Distributed Systems
- Internet and Mobile Security
- Systems and Storage Security
- Usable Security
- Positive and Negative Applications of Artificial Intelligence in Security and Anomaly Detection
- Secure and Trusted AI Systems

3. Academics

Dr. Taheri's laboratory will investigate development of cybersecurity science and related innovative technologies that transform the design and security assessment of large and small enterprises as well as critical applications, such as healthcare systems, power grid systems, financial systems, military systems, transportation systems, and etc. Its education program will include various modules, such as seminar series, tutorials, short courses, educational tools and software, and lecture videos. The center will provide unique learning opportunities in cybersecurity for graduate, undergraduate, and even high school students along with certain entities from enterprises. There will also be specific plans for underrepresented trainees. Meanwhile, there are a number of required courses for the graduate-level researchers that will be offered by the faculty member:

- Computer Architecture Track: (1) Computer System and Software; *and* (2) Advanced Computer Architecture.

- VLSI Track: (1) VLSI Testing and Verification; *and* (2) Advanced VLSI Design.

- Cybersecurity Track: (1) Hardware Security; *and/or* (2) Introduction to Security Aspects of AI.

4. Prospective Students

Dr. Taheri's laboratory will actively seeking highly motivated, skilled, versatile, adept, learner, thinker, creative, and self-driven postdoctoral fellow, graduate and undergraduate students, and visiting researchers with technical and analytical skills for conducting state-of-the-art research in the areas of interests. Candidates with a doctoral or master's degree (or a bachelor's degree with outstanding academic credentials) in Electrical Engineering, Computer Engineering, and Computer Science with expertise and experience in successful research will be encouraged to apply. The prospective members should have a demonstrable and solid background in a number of the following cases:

- Programming Languages: C++; Python; and MATLAB.
- Hardware Languages: Verilog HDL; VHDL; HSPICE; and Assembly.
- Hardware Software Tools: Synopsys, Cadence, and Xilinx Suites; GEM5; and SST.
- AI Software Libraries: TensorFlow; PyTorch; Scikit-learn; Matplotlib; NumPy; OpenCV; Keras; and TensorBoard.
- Operating Systems: Linux.

If you are interested in joining the center, please send a copy of your resume along with any other supporting document(s), all in PDF format to Dr. Taheri.

5. Facilities

The laboratory will include the advanced scientific equipment and software tools for conducting world-leading research on the areas of interest:

- High-End PC Workstations with Linux (Ubuntu) Operating System
- Synopsys, Cadence, and Xilinx Software Suites
- Lambda Quad 4-GPU Deep Learning Workstation

6. Outreach: The outreach items are stated as Research Conference, Forum, Distinguished Speakers, Student Organization, Academic Outreach, Research Experience for Undergraduate (REU) Program, Course-based Undergraduate Research Experience (CURE) Program, YouTube Channel, and Laboratory Tours.

7. Sponsors

Dr. Taheri's center will look for funding opportunities from the following agencies, institutions, and companies: Advanced Micro Devices, Air Force Office of Scientific Research, AmerisourceBergen Corporation, Apple Inc., Cisco, Comcast Corporation, Dell, Department of Commerce, Department of Defense, Department of Energy, Hewlett-Packard Company, Intel Corporation, International Business Machines Corporation, Lockheed Martin Corporation, Meta Platforms, Microsoft Corporation, National Aeronautics and Space Administration (NASA), National Institute of Standards and Technology, National Science Foundation, Nvidia Corporation, Pennsylvania Department of Community and Economic Development, Pennsylvania Department of Labor and Industry, PNC Financial Services Group Inc., Qualcomm, Robert Bosch GmbH, Rockwell Automation, Samsung Electronics Co., Taiwan Semiconductor Manufacturing Company, Texas Instruments, U.S. Army, and Xilinx.

8. Media: The media items are Newsletter and Press.

9. Publications: Please refer to the Dr. Taheri's Google Scholar webpage.