**CMC Research Workshop: Secure IoT Hardware Presentation and Speaker Info**

---

**Presentation:** *Hardware Trojan War!*
**Speaker:** Dr. Mitra Mirhassani, PhD, PEng, SMIEEE: Associate Professor and Co-Director, SHIELD Automotive Cybersecurity Centre of Excellence
**Organization:** University of Windsor

**Abstract:** This presentation goes over some of the problems associated with the integrity of the silicon supply chain.

**Bio:** Mitra Mirhassani is an associate professor at the Electrical and Computer Engineering Department at the University of Windsor. Her research interests include hardware security, Trojan detection, and quantum-safe encryption.

She and her team are investigating a range of hardware security issues such as detecting malicious Trojan Hardware, Efficient implementation of Post-Quantum Algorithms, and implementation of Public Unclonable Functions.

Mitra Mirhassani is a senior member of IEEE and is serving as the Associate Editor for IEEE Access Journal and Guest Associate Editor of IEEE Transaction on Computer-Aided Design. She is the co-founder and co-director of the SHIELD- Automotive Cybersecurity Centre of Excellence.

She was the advisor to the WiCyS (Women in Cybersecurity) Windsor chapter in 2019, and won the leadership award for the groups' activity in promoting the field in 2020. She was recognized as one of the Top Women in Cybersecurity by IT World Canada in 2020 and won the 2020 Outstanding Achievement award, and Leadeship award in cybersecurity in 2021 from the APMA Cybersecurity Institute.

---

**Presentation:** *Detection is Not Enough: Low Cost Attack Recovery for Robotic Vehicle Systems*
**Speaker:** Dr. Karthik Pattabiraman: Professor, Electrical and Computer Engineering
**Organization:** University of British Columbia

**Abstract:** Autonomous Robotic Vehicles (RV) such as drones and rovers rely extensively on sensor measurements to perceive their physical states and the environment. For example, a GPS provides geographic position information, a gyroscope sensor measures angular velocities, an accelerometer measures linear accelerations. Attacks such as sensor tampering and spoofing can feed erroneous sensor measurements through external means that may deviate RVs from their course and result in mission failures. Attacks such as GPS spoofing have been performed against military drones and marine navigation systems. Prior work in the security of

autonomous RVs mainly focuses on attack detection. However, detection alone is not enough, because it does not prevent adverse consequences such as drastic deviation and/or crash. The key question, "how to respond once an attack is detected in an RV?" still remains unanswered. In this talk, I'll describe some of the approaches we've been pursuing in my group to address this question, and our future directions.

**Bio:** Karthik Pattabiraman is a Professor of Electrical and Computer Engineering at the University of British Columbia (UBC). He received his MS and PhD from the University of Illinois at Urbana Champaign (UIUC) in 2004 and 2009, and spent a postdoctoral year at Microsoft Research (MSR), Redmond before joining UBC in 2010. His research interests are in dependability, security, and software engineering. Karthik has won multiple awards such as the Inaugural Rising Star in Dependability Award, 2020, from the IEEE and IFIP, the distinguished alumnus award from the University of Illinois (UIUC), CS department, 2018, and three awards for excellence in research and mentoring from UBC. He is a senior member of the IEEE, a distinguished member of the ACM, and a vice-chair of the IFIP Working Group on dependable computing and fault-tolerance (WG 10.4). A more detailed biography may found at: https://blogs.ubc.ca/karthik/about/full-bio/

---

**Presentation:** *Reliable Machine Learning Resistant Physically Unclonable Functions*
**Speaker:** Dr. Manoj Sachdev: Professor and Interim Department Chair, Electrical and Computer Engineering
**Organization:** University of Waterloo

**Abstract:** Internet of Things (IoT) is enabling networking of billions of devices world-wide. With limited computing resources, such devices often lack mechanisms for secure authentication. Physical Unclonable Functions (PUFs) are a class of low-area/energy circuits that harvest intra/inter-die process variations to generate a device die-specific fingerprint. In this talk, we will review the state of the art, and share some of the ongoing research on how to make PUFs more reliable and machine learning resistant.

**Bio:** Manoj Sachdev is a Professor and Interim Department Chair in the Department of Electrical and Computer Engineering at the University of Waterloo. His research interests include low-power and high-performance digital circuit design, mixed-signal circuit design, test and manufacturing issues of integrated circuits. He has contributed to over 230 conference and journal publications, and has written 5 books and holds more than 30 granted US patents. He is Fellow of IEEE, and Fellow of Canadian Academy of Engineers.

**Presentation:** *Open Problems in Embedded Hardware Security*
**Speaker:** Dr. Colin O'Flynn: Chief Technology Officer
**Organization:** NewAE Technology, Inc.

**Abstract:** Attacks on embedded systems differ greatly than the attacks we consider in classical computers and networks as embedded systems must remain resilient against attacks even with extended physical access. A short summary of relevant hardware-level attacks is presented, with an emphasis on those that have been of concern to industry (often due to their use in real attacks). For these attacks descriptions of some of the open problems are summarized, ranging from questions around ASIC implementations of cryptographic accelerators to machine learning on the analysis data.

**Bio:** Colin obtained a PhD in electrical engineering from Dalhousie University in 2017. During his PhD, Colin started NewAE Technology which worked to make tools for embedded security more available to both academia and industry. After his PhD he also worked as an assistant professor in cybersecurity, and has published both academic and industrial articles on the topic of embedded security (including both conference and journal papers, granted patents, and one book). He has been on numerous program committees for academic conferences (CHES, COSADE, CARDIS, FDTC), given presentations at industry events (such as DEFCON, Blackhat, RECON), and is on the Canadian ISO mirror committee for information security (SC27). His past experience beyond this security-focus includes embedded system design, IoT wireless protocol development, FPGA design, and PCB design and layout.

---

**Presentation:** *Post-Quantum IoT Security*
**Speaker:** Dr. Seokbum Ko: Department Head & Professor, Electrical and Computer Engineering
**Organization:** University of Saskatchewan

**Abstract:** Providing end-to-end security is vital for every network. By emerging quantum computers, it is necessary to design crypto-systems that are secure against quantum attacks. In this presentation, we will introduce several PQC methods and the design of cryptosystems

**Bio:** Dr. Seokbum Ko is currently a Professor and Acting Head at the Department of Electrical and Computer Engineering and a Professor at the Division of Biomedical Engineering, University of Saskatchewan, Canada. He got his PhD degree from the University of Rhode Island, USA in 2002.

His research interests include computer architecture/arithmetic, efficient hardware implementation of compute-intensive applications, deep learning processor architecture and biomedical engineering.

He is a senior member of IEEE circuits and systems society, a member of IEEE VLSI Systems and Application Technical Committee and associate editors of IEEE Transactions on Circuits and Systems I, IEEE Transaction on VLSI and IEEE Access.

---

**Presentation:** *Towards securing hardware in the presence of fault attacks*
**Speaker:** Dr. Catherine Gebotys, Professor: Electrical and Computer Engineering
**Organization:** University of Waterloo

**Abstract:** Recently Electro-Magnetic (EM) Fault Injection techniques have been found to have significant implications on the security of embedded devices. Unfortunately, there is still a lack of understanding of EM faults and countermeasures for embedded processors. This talk will briefly review the importance of fault injection attacks, including recent results on RISC-V, and discuss a strategy for defending against them. This research aims to enhance the understanding of faults, in order to better design countermeasures for embedded processors resistant to fault injection attacks.

**Bio:** Catherine Gebotys is currently a Professor in the Department of Electrical and Computer Engineering at the University of Waterloo. She is the author of 'Security in Embedded Devices', Springer, 2010, sole inventor of several patents and has widely published in the area of embedded systems security (fault injection (EM/laser) attacks/countermeasures, side channel (photonics/power/electromagnetic) analysis).

---

**Presentation:** *SoC/FPGA Cybersecurity Strategies*
**Speaker:** Prof. Amine Miled
**Organization:** Université Laval

**Abstract:** This presentation addresses some security aspects of emerging Systems on a Chip (SoC) Field Programmable Gate Array (FPGA) devices. Unlike standalone FPGAs, primarily composed of malleable logic blocks, SoC FPGAs incorporate a hard processing system (HPS) intricately connected with the FPGA. By integrating both the HPS and the FPGA within the same die, SoC FPGAs can route signals between the processor and the FPGA logic internally, thus reducing the need for external signals. Nevertheless, most SoC FPGAs still require one to load configuration files from external sources. These potentially sensitive files remain vulnerable while outside the device. For this reason, as available for standalone FPGAs, manufacturers provide the ability to encrypt and authenticate these files. Other security features common to most standalone FPGAs and SoC FPGAs include the ability to disable the device's debug access ports and configuration readback. However, the HPS in SoC FPGAs adds a level of complexity that is not present for standalone FPGAs. This added complexity necessarily hands over the task of securing the device

to the developers. Even with standard security features, the HPS might still have unhindered access to the FPGA logic. A single software flaw could open up a breach that might allow an attacker to reach the FPGA logic via the supposedly trusted HPS-FPGA interface. Developers working on SoC FPGAs, therefore, need a robust strategy when implementing cybersecurity within their designs.

**Bio:** Prof. Amine Miled received his Ph.D. degree from École Polytechnique de Montréal, in Québec, Canada, in 2013. In 2013, he joined the Electrical and Computer Engineering Department at Laval University in Quebec City, Canada, where he is associate professor and member of the Radio communications and Signal Processing Laboratory. He is also the director of LABioTRON Bioengineering research laboratory at the Electrical and Computer Engineering Department at Laval University.Prof. Miled Interests are mainly on microelectronics (Integrated Circuit Design), microfluidics, microfabrication and microsystem design for biomedical applications. He is focusing on the development of miniaturized Lab-on-Chip for neurotransmitter sensing and manipulation for neurodegenerative diseases. His research topics also cover other applications such as water and air quality monitoring. His research is multidisciplinary going from multiphysics modeling with FEM to Packaging of Hybrid technologies and advanced microfabrication for microfluidic and high throughput microelectrode array and cybersecurity.