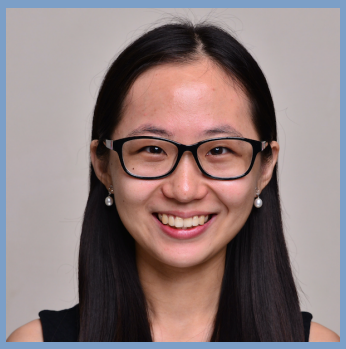


XIAOLU HOU

Faculty of Informatics and Information Technologies
Slovak University of Technology

Project number
2130/01/01

Project duration
10/2021 - 9/2024

"I applied for SASPRO 2 programme because it provides me with an excellent opportunity to pursue my own research in one of the top research institutes in Slovakia. The planned research will enhance my experience in both hardware security as well as neural network security. Those experiences will aid in my academic career. Project management and leadership skills obtained will strengthen my competence in my pursuit of a professorship. Scientific achievements during the fellowship, such as publications at renowned venues, and the establishment of collaborations with various research organizations within Europe will help me in starting my academic career in the EU area and will give me a good initial position for the beginning phases of my professorship."

BIOGRAPHY

Xiaolu Hou received her Ph.D. degree in mathematics from Nanyang Technological University (NTU), Singapore, in 2017. Her research focus is on fault injection and sidechannel attacks. She also has research experience in security of neural networks, location privacy, multiparty computation, and differential privacy. With a wide range of research interests, she has published her work at top venues within various fields, ranging from mathematics to computer security.

PROJECT SUMMARY

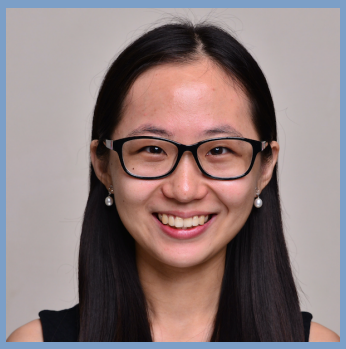
Hardware Security of Neural Networks – HARSONN

Decision-making tasks carried out by the usage of neural networks are successfully taking over in many areas, including those that are security-critical, such as healthcare, transportation, smart grids, where intentional and unintentional failures can be disastrous. Neural network implementations rely on hardware platforms (e.g., FPGAs, GPUs, and microcontrollers) to accelerate the computations. These physical systems are vulnerable to physical attacks, as has been demonstrated in the domain of applied cryptography, where the attacks have been carried out to mount the secret key recovery or for violating/bypassing security checks. Therefore, there is a necessity to evaluate the potential attacks that can target neural networks on the hardware level.

In this project, we focus on two major hardware-level attacks on neural networks that were well studied for cryptographic implementations before – side-channel attacks and fault attacks. Side-channel attacks are passive attacks that observe physical quantities related to the computation of sensitive variables and exploit them to gain unauthorized information. Fault attacks are active attacks that disrupt the device during the computation to provide benefit for the attacker.

The goal of the project is to investigate possible attack vectors and propose countermeasures on all aspects of neural network development (training data, training program, deployed network). We will first conduct a comprehensive study on the current attack methods and countermeasures. Next, we will develop novel attacks and suggest possible countermeasures. Our results can serve as a basis to outline the susceptibility of neural networks to physical attacks which can be considered a viable attack vector whenever a device is deployed in a hostile environment.

SASPRO 2



XIAOLU HOU

Faculty of Informatics and Information Technologies
Slovak University of Technology

Project number
2130/01/01

Project duration
10/2021 -9/2024

PUBLICATIONS

1. Won, Yoo-Seung, **Xiaolu Hou,** Dirmanto Jap, Jakub Breier, and Shivam Bhasin. "Back to the basics: Seamless integration of side-channel pre-processing in deep neural networks." IEEE Transactions on Information Forensics and Security 16 (2021): 3215- 3227. [PDF]

2. Breier, Jakub, **Xiaolu Hou,** and Yang Liu. "On evaluating fault resilient encoding schemes in software." IEEE Transactions on Dependable and Secure Computing 18, no. 3 (2019): 1065-1079. [PDF]

3. Breier, Jakub, Mustafa Khairallah, **Xiaolu Hou,** and Yang Liu. "A countermeasure against statistical ineffective fault analysis." IEEE Transactions on Circuits and Systems II: Express Briefs 67, no. 12 (2020): 3322-3326. [PDF]

4. Breier, Jakub, Dirmanto Jap, **Xiaolu Hou,** and Shivam Bhasin. "On side channel vulnerabilities of bit permutations in cryptographic algorithms." IEEE Transactions on Information Forensics and Security 15 (2019): 1072-1085. [PDF]

5. Breier, Jakub, **Xiaolu Hou,** Dirmanto Jap, Lei Ma, Shivam Bhasin, and Yang Liu. "Practical fault attack on deep neural networks." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 2204-2206. 2018. [PDF]

S A S P R O 2

STU

COMENIUS UNIVERSITY BRATISLAVA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 945478.