YANNAN LIU (刘彦南)

Shenzhen, China
Email: lyn240690234@gmail.com
Tel: (+86) 13128813658

EDUCATION

- The Chinese University of Hong Kong — Aug. 2013 - Aug. 2017
  PhD. in Computer Science and Engineering

- Zhejiang University — Sep. 2008 - Jun. 2012
  B.Eng. in Computer Science and Technology

RESEARCH INTEREST

Cyber security, malware detection and analysis, binary analysis, hardware security, computer system security, deep learning, internet of things, computer architecture.

EXPERIENCE

- Security Technical Expert
  Sangfor Technologies Inc., Research Innovation Institution — Sep. 2017- Present

- Research Assistant
  The Chinese University of Hong Kong, CSE Department — Aug. 2012 - Jul. 2013

- Teaching Assistant

CSCI2100A Data Structure	2013-2014 Fall
CENG3420 Computer Organization and Design	2013-2014 Spring
CMSC5719 Seminar Course	2014-2015 Fall
ENGG2020 Digital Logic and Systems	2014-2015 Fall
CENG3420 Computer Organization and Design	2014-2015 Spring
ENGG2020 Digital Logic and Systems	2015-2016 Fall

SELECTED PROJECTS

- Sangfor AI-based Vanguard Engine (SAVE) Sep. 2017 – Present
  - Lead the R&D of AI-based malware detection capability in SAVE, including feature engineering of multiple file types, malware detection, malware family classification, AI-aware detection architecture and so on.
  - Lead the R&D of backend malware analysis platforms, e.g., executable binary similarity analysis platform and NLP-based familial label platform.
  - Lead the R&D of SAVE AI capability deployment in multiple product lines (EDR, AF, SIP).
  - Lead the R&D of POC program for SAVE AI capability.

- Differential Fault Attack Jan. 2014 - Feb. 2015
  - Propose error rate analysis and design a new sskey extractor.
  - Propose a new flexible and efficient differential fault attack method.
  - Demonstrate proposed attack with AES cipher on FPGA platform.

- Code Execution Tracking via Power Side-Channel Mar. 2015 - Feb. 2016
  - Propose a method to track the normal instruction execution on MCU via power side-channel.
  - Propose a method to detect abnormal execution via power side-channel.
  - Revise hidden Markov model and Viterbi algorithm to improve tracking efficiency.
  - Design a signal extraction method to mitigate the noise in power side-channel.

- Deep Learning Security Jul. 2016 – Feb. 2017
  - Propose fault injection attack for deep neural network, and design two attack methods.
  - Study deep neural network's power side-channel leakage.
  - Investigate the adversarial example problem during neural network compression.

PUBLICATIONS

- Conference

[15] **Yannan Liu**, Yabin Lai, Kaizhi Wei, Liang Gu, and Zhengzheng Yan, "NLabel: An Accurate Familial Clustering Framework for Large-scale Weakly-labeled Malware", accepted by 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (**TrustCom**), 2020. (CCF C)

[14] Yu Li, **Yannan Liu**, Min Li, Ye Tian, Bo Luo, and Qiang Xu. "D2NN: a fine-grained dual modular redundancy framework for deep neural networks.", 35th Annual Computer Security Applications Conference (**ACSAC**), 2019. (CCF B)

[13] Xian Zhang, Guangyu Sun, Peichen Xie, Chao Zhang, **Yannan Liu**, Lingxiao Wei, Qiang Xu, and Chun Jason Xue. "Shadow Block: Accelerating ORAM Accesses with Data Duplication", IEEE/ACM International Symposium on Microarchitecture (**MICRO**), 2018. (CCF A)

[12] Lingxiao Wei, Bo Luo, Yu Li, **Yannan Liu**, and Qiang Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators", Computer Security Applications Conference (**ACSAC**), 2018. (CCF B)

[11] Bo Luo, **Yannan Liu**, Lingxiao Wei, and Qiang Xu, "Towards imperceptible and robust adversarial example attacks against neural networks", AAAI Conference on Artificial Intelligence (**AAAI**), 2018. (CCF A)

[10] **Yannan Liu**, Liangxiao Wei, Bo Luo, and Qiang Xu, "Fault injection attack on deep neural network", IEEE/ACM International Conference on Computer-Aided Design (**ICCAD**) 2017. (CCF B)

[9] Ting Wang, **Yannan Liu**, Qiang Xu, Zhaobo Zhang, Zhiyuan Wang and Xinli Gu, “RetroDMR: Troubleshooting NonDeterministic Faults with Retrospective DMR", IEEE/ACM Design, Automation, and Test in Europe (**DATE**), 2017, (Accepted for Publication as an Interactive Presentation). (CCF B)

[8] **Yannan Liu**, Lingxiao Wei, Zhe Zhou, Kehuan Zhang, Wenyuan Xu, Qiang Xu, “On Code Execution Tracking via Power Side-Channel", ACM Conference on Computer and Communications Security (**CCS**) 2016. (CCF A)

[7] Lingxiao Wei, Chaosheng Song, **Yannan Liu**, Jie Zhang, Feng Yuan, Qiang Xu, “BoardPUF: Physical Unclonable Functions for Printed Circuit Board Authentication", IEEE/ACM International Conference on Computer-Aided Design (**ICCAD**) 2015. (CCF B)

[6] **Yannan Liu**, Jie Zhang, Lingxiao Wei, Feng Yuan and Qiang Xu, “DERA: Yet Another Differential Fault Attack on Cryptographic Devices Based on Error Rate Analysis", ACM/IEEE Design Automation Conference (**DAC**) 2015. (**Nominated for Best Paper Award**) (CCF A)

[5] Lingxiao Wei, Jie Zhang, Feng Yuan, **Yannan Liu**, Junfeng Fan, Qiang Xu, “Vulnerability Analysis for Crypto Devices against Probing Attack", IEEE/ACM Asia and South Paci c Design Automation Conference (ASP-DAC) 2015. (CCF C)

[4] Jie Zhang, Guantong Su, **Yannan Liu**, Lingxiao Wei, Feng Yuan, Guoqiang Bai, Qiang Xu, “On Trojan Side Channel Design and Identification", IEEE/ACM International Conference on Computer-Aided Design (**ICCAD**) 2014. (CCF B)

[3] Feng Yuan, **Yannan Liu**, Wen-Ben Jone, Qiang Xu, “On testing timing-speculative circuits", ACM/IEEE Design Automation Conference (**DAC**) 2013. (CCF A)

[2] **Yannan Liu**, Tianzhou Chen, Tiefei Zhang, Jinming Yue, “Dealing with the Functional Units Starvation in SMT", IEEE International Conference on High Performance Computing and Communication & IEEE International Conference on Embedded Software and Systems (HPCC-ICESS) 2012.

[1] Jinming Yue, Tiefei Zhang, **Yannan Liu**, Baixing Quan, Tianzhou Chen, “Thermal-Aware Feedback Control Scheduling for Soft Real-time Systems", IEEE International Conference on High Performance Computing and Communication & IEEE International Conference on Embedded Software and Systems (HPCC-ICESS), 2012.

- Journal

[1] Jie Zhang, Feng Yuan, Lingxiao Wei, **Yannan Liu**, Qiang Xu, “VeriTrust: Veri cation for Hardware Trust", IEEE Trans. on CAD of Integrated Circuits and Systems (TCAD). (CCF A)