YI HAN

Email:hcheerment@gmail.com

RESEARCH INTEREST

I have experience applying deep learning/machine learning techniques to computer system security applications such as control flow monitoring, vulnerability detection and malware detection. I also worked on evaluating the robustness of deep learning/machine learning systems. My research interests include computer security, machine learning and signal processing.

PUBLICATIONS

Top tier security conference:

Yi Han, Matthew Chan, Zahra Aref, Nils Ole Tippenhauer, Saman Zonouz. "Hiding in Plain Sight? On the Efficacy of Power Side Channel-Based Control Flow Monitoring", 31th USENIX Security Symposium (USENIX Security 22). 2022.

Yi Han, Sriharsha Etigowni, Hua Liu, Saman Zonouz, Athina Petropulu, "Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations", ACM Conference on Computer and Communications Security (CCS), October 2017.

Top signal processing journal:

Yi Han, Ioannis Christoudis, Kostas Diamantaras, Saman Zonouz, Athina Petropulu, "Side-Channel-Based Code-Execution Monitoring Systems - A Survey", IEEE Signal Processing Magzine, vol. 36, no. 2, pp. 22-35, March 2019.

Others:

Xu, Zhichao, **Yi Han**, Yongfeng Zhang, and Qingyao Ai. "E-commerce Recommendation with Weighted Expected Utility", Proceedings of the 29th ACM International Conference on Information and Knowledge Management (CKIM), October 2020.

Pengfei Sun, Luis Garcia, **Yi Han**, and Saman Zonouz, Yao Zhao. "Poster: Known Vulnerability Detection forWebAssembly Binaries", 2021 IEEE Symposium on Security and Privacy (SP) Posters. IEEE, 2021.

EXPERIENCES

Shape Security - Research Intern — May 2020 - August 2020

Samsung Research America - Research Intern — June 2018 - August 2018

PROJECT/RESEARCH EXPERIENCE

Physical Adversarial Attack against Image Recognition and Object Detection Systems
Rutgers University

- Designed a physical adversarial attack approach against image classification/recognition cameras by attaching a transparent display on to a victim camera
- Designed an optimization approach to generate universal adversarial perturbation (UAP) images to be displayed on the transparent display

- Experiments on traffic signs shows the proposed attack can mislead traffic sign classification/recognition camera with high attack success rate (ASR)

Malicious JavaScript Detection
Shape Security Inc.

- Designed a Malicious JavaScript Detection system based on both static and dynamic analysis
- Static analysis - Extract syntactic and semantic features from JavaScript Code and train a Random Forrest Classifier to distinguish between malicious and benign code
- Dynamic analysis - Instrument the JavaScript code, perform API tracing and taint analysis to identify malicious activities

Adversarial Robustness of Machine Learning based Side Channel Control Flow Monitoring Systems
Rutgers University

- Identified the weakness of machine learning based side channel control flow monitoring systems against adversarial perturbations
- Proposed an attack framework against the monitoring system: designed a Monte Carlo Tree search (MCTs) based optimization framework to find the optimal way of injecting the malicious code such that the injected program can bypass the monitoring system

Source Code Level Vulnerability Detection Using Deep Learning
Samsung Research America

- Designed a source code level vulnerability detection system using bidirectional recurrent neural network (BiRNN)
- Added attention mechanism to the BiRNN model and used the attention map to further locate the vulnerable spots in the code

Neural Network based Profiling Attack against AES via Power Side Channel
Rutgers University

- Collect power side channel signals from a STM32F3 Micro-controller running an AES encryption program
- Profiled the encryption process by designing a convolution neural network (CNN) model to map power side channel signals to their corresponding hamming weight of the output of the SBOX replacement operation in the 1st round
- Designed a maximum likelihood hypothesis testing framework based on the output distribution of the CNN model to verify the key byte guesses and thus recover the secret key

Program Control Flow Integrity Monitoring using Neural Network
4N6 lab and CSPL lab in Electrical and Computer Engineering, Rutgers University

- Designed a sensing system to capture unintentional electromagnetic emanation from programmable logic controllers (PLCs)
- Proposed a program behavior model that is based on the electromagnetic emanation, using long short-term memory (LSTM) neural network layers
- Proposed a control flow monitoring and intrusion detection framework based on the behavior model
- Evaluated the framework against popular control flow attacks, such as control flow hijacking, code injection and code reuse etc.

EDUCATION

Rutgers University September 2015 - Present
Ph.D in Electrical and Computer Engineering
GPA: 3.9/4.0

Xidian University September 2011 - June 2015
B.S. in Electronic Information Engineering
GPA of Major courses: 87.5/100

COURSE

Rutgers University

- Malware Analysis and Reverse Engineering
- Biomedical Image Processing and Recognition
- Pattern Recognition and its Applications (Unsupervised learning)
- Biometrics (Machine learning approaches to biometric authentication)
- Detection and Estimation Theory

Xidian University

- Digital Image Processing
- Pattern Recognition

TECHNICAL STRENGTH

Computer Languages	Python, C, C++ Assembly
Frameworks	Anaconda, Tensorflow, Pytorch
Hardware	Power & electromagnetic signal sensing, Embedded system