SANCHUAN CHEN

Mailing address: 18 Engle St Apt 9D, Tenafly, New Jersey, 07670
Phone: 614-364-1704 ⋄ Email: schen409@fordham.edu ⋄ Website: https://schuan.github.io/

Professional Experience

Fordham University Sep. 2021 - Present
Tenure-track Assistant Professor
Department of Computer and Information Sciences

The Ohio State University Aug. 2018 - Aug. 2021
Graduate Research Assistant
Department of Computer Science and Engineering

Education

The Ohio State University Aug. 2014 - Aug. 2021
Ph.D. in Computer Science and Engineering
Thesis: Exploring Value Set Analysis for Binary Code Hardening and Vulnerability Detection
Advisors: Dr. Zhiqiang Lin and Dr. Yinqian Zhang
Committee: Dr. Zhiqiang Lin, Dr. Yinqian Zhang, Dr. Michael D. Bond, Dr. Atanas Rountev

Institute of Software, Chinese Academy of Sciences Aug. 2009 - Jan. 2014
M.E. in Computer Software and Theory

University of Science and Technology of China Aug. 2005 - July 2009
B.E. in Computer Software and Technology

Research Interests

Software Security
Programming Languages
Trusted Execution Environment
Artificial Intelligence

Research Publications

Controlled Data Races in Enclaves: Attacks and Detection
Sanchuan Chen, Zhiqiang Lin, Yinqian Zhang.
USENIX Security'23, Anaheim, CA, USA, Aug. 2023.

SelectiveTaint: Efficient Data Flow Tracking With Static Binary Rewriting
Sanchuan Chen, Zhiqiang Lin, Yinqian Zhang.
USENIX Security'21, Vancouver, B.C., Canada, Aug. 2021.

SgxPectre: Stealing Intel Secrets from SGX Enclaves via Speculative Execution
Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten H. Lai.
EuroSP'19, Stockholm, Sweden, Jun. 2019. Cited 406 times.

Leveraging Hardware Transactional Memory for Cache Side-Channel Defenses
Sanchuan Chen, Fangfei Liu, Zeyu Mi, Yinqian Zhang, Ruby B. Lee, Haibo Chen and XiaoFeng Wang.
AsiaCCS'18, Incheon, Korea, June 2018.

Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races
Guoxing Chen, Wenhao Wang, Tianyu Chen, Sanchuan Chen, Yinqian Zhang, XiaoFeng Wang, Ten-Hwang Lai, Dongdai Lin.
Oakland'18, San Francisco, USA, May. 2018. Cited 70 times.

Stacco: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves
Yuan Xiao, Mengyuan Li, Sanchuan Chen, Yinqian Zhang .
CCS'17, Dallas, USA, Oct. 2017. Cited 63 times.

Detecting Privileged Side-Channel Attacks in Shielded Execution with DÉJÀ VU
Sanchuan Chen, Xiaokuan Zhang, Michael K. Reiter, Yinqian Zhang.
AsiaCCS'17, Abu Dhabi, UAE, Apr. 2017. Cited 208 times.

Research Experience

Detecting Controlled Data Races in Enclave Code
The project investigates a novel attack vector of Intel SGX, which is caused by non-reentrant enclave code that allows an attacker to trigger a controlled data race, and proposes a static binary analysis tool to detect controlled data races in enclave executables.

Improving Performance of Data Flow Tracking
The project proposes the first framework leveraging value set analysis to selectively instrument data flow tracking into binary code with static binary instrumentation instead of dynamic binary instrumentation.

Detecting Privileged Side Channel Attacks in Shielded Execution
The project presents a software framework that enables a shielded execution to detect privileged side-channel attacks and builds into shielded execution the ability to check its own basic block execution time.

Detecting Cross-Architecture Binary Similarity
The project uses architecture-neutralized and optimization-resilient value sets of each registers and memory cells at function exit point as a signature to capture the semantics of a function for similarity comparison.

Detecting Kernel Vulnerabilities with Machine Learning
This ongoing project leverages machine learning techniques to advance software security research, particularly, vulnerability detection in Linux kernel code.

Improving Correctness of Deep Learning Compilers
This ongoing project uses program testing and program analysis techniques to improve the correctness of deep learning compilers.

Research Grant Experience

Using Program Analysis for Blockchain System Education — Mar. 2022
Requested budget: $5,000 + $2,000 summer student fees
Fordham University Faculty Research Grant

Type-aware recovery of symbol names in binary code: a machine learning based approach	Mar. 2021
Requested budget: $80,000 + $20,000 credits	
Amazon Research Award, Compilation Associate	

Research Mentoring Experience

Mentored the research of three graduate students and five undergraduate students:

Xueqing Zhang, Arna Sadia, Ujjwal Samanta (MS, Fordham)
Chen Ling, Shurav Nandy, Tianshi Zhang (BS, Fordham)
Andrew Haberlandt, Bo Lu (BS, OSU)

Teaching Experience

Instructor, Fordham University	Spring 2022, Spring 2023
CISC 4090: Theory of Computation	30 students, 2 terms
Instructor, Fordham University	Autumn 2021, Spring 2022, Autumn 2022, Spring 2023
CISC 3500: Database Systems	30 students, 4 terms
Lab Instructor, OSU	Aug. 2015 - May 2017
CSE 2111: Modeling and Problem Solving with Spreadsheets and Databases	200 students, 6 terms
Graduate Teaching Assistant, OSU	Aug. 2014 - May 2015
CSE 5331: Foundations II: Data structures and algorithms	40 students, 2 terms

Service Experience

Program Committee

EAI International Conference on Security and Privacy in Communication Networks(SecureComm)	2022
IEEE International Conference on Parallel and Distributed Systems (ICPADS)	2022
International Conference on Information Security and Cryptology (Inscrypt)	2022

Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)	2020
Journal of Computer Science and Technology (JCST)	2021
Journal of Cybersecurity and Privacy (JCP)	2022
Forensic Science International: Digital Investigation	2021
Applied Sciences	2022
Future Internet	2021
PLOS ONE	2021, 2022

Shadow Program Committee

IEEE Symposium on Security and Privacy (Oakland)	2021

External Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)	2019
IEEE Symposium on Security and Privacy (Oakland)	2017, 2021, 2022
ACM Conference on Computer and Communications Security (CCS)	2017, 2018, 2020, 2022

USENIX Security Symposium (SEC)	2017, 2021, 2022
ISOC Network and Distributed System Security Symposium (NDSS)	2019, 2020
European Symposium on Research in Computer Security (ESORICS)	2021
Annual Computer Security Applications Conference (ACSAC)	2018, 2019, 2020
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2021
International Conference on Dependable Systems and Networks (DSN)	2020, 2021
EAI International Conf. on Security and Privacy in Communication Networks(SecureComm)	2019, 2020
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	2019
International Conference on Applied Cryptography and Network Security (ACNS)	2020
Annual Digital Forensics Research Conference (DFRWS)	2019

Artifact Evaluation Committee

Annual Computer Security Applications Conference (ACSAC)	2020

Media Coverage

Received wide media coverage and selected pieces are:

“New Spectre attack variant can pry secrets from Intel’s SGX protected enclaves”
by Liam Tung, ZDNet, March 2, 2018.(Link)

“Spectre-like attack exposes entire contents of Intel’s SGX secure enclave”
by James Sanders, TechRepublic, March 5, 2018.(Link)

“New Spectre derivative bug haunts Intel processors”
by Andy Patrizio, Network World, March 7, 2018.(Link)

“Spectre haunts Intel’s SGX defense: CPU flaws can be exploited to snoop on enclaves”
by Richard Chirgwin, The Register, March 1, 2018.(Link)

“If there’s somethin’ stored in a secure enclave, who ya gonna call? Membuster!”
by Thomas Claburn, The Register, December 5, 2019.(Link)

Awards

Faculty Research Grant, Fordham University	2022
Student Travel Grant, AsiaCCS 2018	2018
Excellent Volunteer of 50th Anniversary of USTC, USTC	2008
Outstanding Student Scholarship Grade 2, USTC	2008
Outstanding Student Scholarship Grade 2, USTC	2007
Outstanding Student Scholarship Grade 3, USTC	2006
Outstanding Freshman Scholarship Grade 3, USTC	2005