SANCHUAN CHEN

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

WORK EXPERIENCE

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

EDUCATION

The Ohio State University *Aug. 2014 - Aug. 2021*
Ph.D. student in Computer Science and Engineering
Department of Computer Science and Engineering
Advisors: Dr. Zhiqiang Lin, Dr. Yinqian Zhang

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

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

RESEARCH INTERESTS

Software Security
Programming Languages
Binary Analysis
Trusted Execution Environment

PUBLICATIONS

SGX-Racer: Detecting Controlled Data Races in Enclave Binaries
Sanchuan Chen, Zhiqiang Lin, Yinqian Zhang.
In submission.

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.
EuroS&P'19, Stockholm, Sweden, Jun. 2019.

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.
AsiaCCS18, 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.

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.

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.

RESEARCH EXPERIENCE

Detecting Controlled Data Races in Enclave Code
The project investigates a new attack vector of Intel SGX, which is caused by non-reentrant enclave code that allows an attacker, e.g., a malicious OS, to trigger a controlled data race to breach the integrity of the enclaves execution and proposes a static binary analysis tool to identify the exploitable data races in enclave executable.

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

Improving Performance of Data Flow Tracking
The project aims at designing novel static binary analysis algorithm to identify instructions that will not be tainted at run-time to improve the performance of data flow tracking system such as libdft.

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 we build into shielded execution the ability to check program execution time at the granularity of paths in its control-flow graph.

RESEARCH GRANT EXPERIENCE

Using Program Analysis for Blockchain System Education *March 2022*
Requested budget: $5,000 + $2,000 summer student fees
Faculty Research Grant (Awarded).

Proposal Drafting:
Type-aware recovery of symbol names in binary code: a machine learning based approach *March 2021*
Requested budget: $80,000 + $20,000 credits
Amazon Research Award (Awarded).

RESEARCH MONTORING EXPERIENCE

Mentored the research of four undergraduate students:

- Shurav Nandy (BS, Fordham)
- Tianshi Zhang (BS, Fordham)
- Andrew Haberlandt (BS, OSU)
- Bo Lu (BS, OSU)

TEACHING EXPERIENCE

Instructor, Fordham *Spring 2022*
CISC 4090: Theory of Computation 30 students, 1 term
Instructor, Fordham *Spring 2022, Fall 2021*
CISC 3500: Database Systems 30 students, 2 terms

SERVICE EXPERIENCE

Program Committee
EAI International Conference on Security and Privacy in Communication Networks(SecureComm) *2022*

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

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 Conference 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

"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)