Mingshen Sun

Ph.D. in System Security, Staff Security Researcher at Baidu X-Lab

1195 Bordeaux Dr
Sunnyvale, CA 94089, USA
+1 408 505 3679
bob@mssun.me
https://mssun.me
https://github.com/mssun
Google Scholar

Experience

Mar., 2017–present **Staff Security Researcher**, *Baidu X-Lab, Baidu USA*, Sunnyvale, USA

Research and development in system security, mobile security, IoT security, TEE, confidential computing, and vehicle security.

- Lead the Apache Teaclave (incubating) project. Teaclave is an open source universal secure computing (confidential computing) platform making computation on privacy-sensitive data safe and simple. Teaclave powers a number of commercial products and open source projects. Its Teaclave (Rust) SGX SDK and Teacalve (Rust OP-TEE) TrustZone SDK are recommended SDKs for SGX and TrustZone development in Rust by Intel and OP-TEE.
- Lead P4Cleanroom, a confidential cloud service for hosting computational biology algorithms as SaaS services on the cloud powered by Teaclave.
- Lead the MesaPy project, a fast and safe Python based on PyPy with SGX support.
- Lead the MesaLock Linux project, a memory-safe Linux distribution.
- Apply secure boot, TrustZone, and user space protection mechanism to IoT devices.
- Research on differential privacy, memory-safety of the Rust programming language, and security of TEE boundary.

Aug., 2019–present. **Podling Project Manamgement Committee (PPMC)**, *Apache Teaclave (incubating)*

PPMC is responsible for the proper management and oversight of the incubating Teaclave project in Apache. Besides design and engineering Teaclave, it also includes managing the Teaclave peoject: roadmap setup, maintaining open source community, organizing activities (meetups), electing and mentoring new members, etc.

Jun.–Sep., 2014 **Research Assistant**, *School of Computing, National University of Singapore*, Singapore

Research and experimental development on behavior-based malware detection system for Android mentored by Prof. Zhenkai Liang and Prof. Richard T.B. Ma.

Jun.–Sep., 2013 **Research Internship**, *Wireless Security Research Department, Qihoo 360*, Beijing, China

Research and experimental development on host-based intrusion prevention system (HIPS) for Android working mentored by Prof. Xuxian Jiang.

- Investigated on existing Android HIPS, discovered vulnerabilities and wrote POC programs. [Demo]
- Designed and prototyped a secure HIPS with dynamic detection feature based on API hooking.

Projects

2019–present **Teaclave: A Universal Secure Computing Platform**, *Lead/Core Developer*, https://teaclave.apache.org

Apache Teaclave (incubating) is an open source universal secure computing platform, making computation on privacy-sensitive data safe and simple. Here are some highlights:

- **Secure and Attestable**: Teaclave adopts multiple security technologies to enable secure computing, in particular, Teaclave uses Intel SGX to serve the most security-sensitive tasks with hardware-based isolation, memory encryption and attestation. Also, Teaclave is written in Rust to prevent memory-safety issues.
- **Function-as-a-Service**: Teaclave is a function-as-a-service platform supports tasks like privacy-preserving machine learning, private set intersection, and crypto computation. In addition, developers can also write and execute Python function. Teaclave supports both general secure computing tasks and flexible multi-party secure computation.
- **Ease of Use**: Teaclave builds its components in containers, therefore, it supports deployment both locally and within cloud infrastructures. Teaclave also provides convenient endpoint APIs, client SDKs and command line tools.
- **Flexibility**: Components in Teaclave are designed in modular, and features like remote attestation can be easily embedded in other projects. In addition, Teaclave SGX SDK and Teaclave TrustZone SDK can also be used separately to write TEE apps for other purposes.

I lead, design, and implement the systems, e.g., attestation, RPC, services, SDK, and maintain the open source community. Now, Teaclave (originally called MesaTEE) has been accepted in Apache Incubator as an open-source governance project. As the PPMC of Tealcave, I maintain the open souce community. This includes roadmap setup, organizing activities, collaborating with external contributors, electing and mentoring new members etc.

Teaclave has been used by many companies' products and open source projects. Please see the powered by page on Teaclave's homepage to learn more.

I also work on finding vulnerabilities in TEE boundary. Here are CVEs found in some popular TEE frameworks: CVE-2020-8904, CVE-2020-8905, CVE-2020-15244, CVE-2020-16966, CVE-2020-8935, CVE-2020-8936, CVE-2020-8937, CVE-2020-8938, CVE-2020-8939, CVE-2020-8940, CVE-2020-8941, CVE-2020-8942, CVE-2020-8943, CVE-2020-8944, CVE-2021-22550, CVE-2021-22549, CVE-2021-22548, CVE-2021-22552.

2018–present **MesaPy: A Fast and Safe Python**, *Lead/Developer*, https://github.com/mesalock-linux/mesapy

MesaPy is a memory-safe Python implementation based on PyPy. In addition to PyPy's distinct features – speed (thanks to the JIT compiler), memory usage, compatibility and stackless (massive concurrency), MesaPy mainly focuses on improving its security and memory safety. On top of the enhancements, we also bring MesaPy into *Intel SGX* to write memory-safe applications running in the trusted execution environment. Right now, MesaPy for SGX becomes one of the main executor of Teaclave.

In this project, We also wrote a book called RPython by Example (RPyBE) which contains a collection of runnable examples that illustrate various RPython concepts and libraries. RPyBE starts with a hello world example and built-in types in RPython, then dives into RPython libraries, writing benchmarks and build a simple application at last.

2019–present **Rust OP-TEE TrustZone SDK**, *Lead/Developer*, https://github.com/apache/incubator-teaclave-trustzone-sdk

Rust OP-TEE TrustZone SDK enables safe, functional, and ergonomic development of trusted apps in Rust. The SDK is based on the OP-TEE project which follows GlobalPlatform TEE API specifications. Additionally, the SDK provides capabilities to write trusted apps with Rust's standard library and many third-party libraries (i.e., crates). Currently, it is a sub-project of Apache Teaclave (incubating).

2017–present **The MesaLock Linux Project**, *Lead/Developer*, https://github.com/mesalock-linux

MesaLock Linux is a general purpose Linux distribution which aims to provide *safe* and *secure* user space environment. To eliminate severe vulnerabilities caused by memory corruption, the whole user space applications are rewritten in memory-safe programming languages like Rust and Go. This extremely reduces attack surfaces of an operating system exposed in the wild, leaving the remaining attack surfaces auditable and restricted. Therefore, MesaLock Linux can substantially improve the security of the Linux ecosystem. Additionally, thanks to the Linux kernel, MesaLock Linux supports a broad hardware environment, making it deployable in many places.

In this project, we also introduce MesaBox, which is a collection of core system utilities written in Rust for Unix-like systems. Like the well-known BusyBox and Toybox sets of utilities popular on embedded devices, MesaBox seeks to provide a fully functioning command-line environment (unlike uutils, which just seeks to reimplement the GNU coreutils).

2018 **YogCrypt: A fast, general purpose crypto library in pure Rust**, *Maintainer*, https://github.com/yogcrypt

YogCrypt is designed to be a high-performance, general purpose crypto library. YogCrypt currently provides three cryptographic algorithms in Chinese National Standard, namely the SM2 cryptographic asymmetric algorithm, the SM3 cryptographic hash algorithm, and the SM4 block cipher algorithm.

2017–present **Pass for iOS**, *Owner*, https://github.com/mssun/passforios

Pass for iOS is an open source password manager written in Swift for iPhone/iPad. The app is compatible with the pass command line tool, which utilizes PGP for encryption/decryption and Git for storage and version control. This repository receives more than 700 stars and has several active contributors on GitHub. In addition, the app has been published in AppStore and received a very high rating (4.8 out of 5) with many positive reviews.

Education

2012–2016 **Ph.D., Computer Science and Engineering**, *The Chinese University of Hong Kong (CUHK)*

interest System Security (Mobile Security), ANSRLab, advised by Prof. John C.S. Lui

thesis Toward a Secure Mobile Platform: From Applications to Systems

2008–2012 **B.S., Computer Science and Technology**, *Northeastern University*, China

gpa & honor 3.6/4.0, 3/394 (major), Provincial Outstanding Graduates, 1 %

Publications

The following is a list of my conference/journal publications in reverse-chronological order. I also actively collaborate with professors and students in universities to conduct various interesting research projects on solving real-world problems in industry.

[1] Jincheng Wang, Zhuohua Li, John C.S. Lui, and **Mingshen Sun**. "Topology-Theoretic Approach To Address Attribute Linkage Attacks In Differential Privacy". In: *Computers & Security* (2022).

[2] Hui Xu, Zhuangbin Chen, **Mingshen Sun**, and Yangfan Zhou. "Memory-Safety Challenge Considered Solved? An Empirical Study with All Rust CVEs". In: *ACM Transactions on Software Engineering and Methodology* (2022).

[3] Zhuohua Li, Jincheng Wang, **Mingshen Sun**, and John C.S. Lui. "MirChecker: Detecting Bugs in Rust Programs via Static Analysis". In: *Proceedings of the 28th ACM Conference on Computer and Communications Security*. CCS '21. Nov. 2021.

[4] Jincheng Wang, Zhuohua Li, John C.S. Lui, and **Mingshen Sun**. "Topology-Theoretic Approach To Address Attribute Linkage Attacks In Differential Privacy". In: *IEEE INFOCOM*

WKSHPS: BigSecurity 2021: International Workshop on Security and Privacy in Big Data. May 2021.

[5] Shengye Wan, **Mingshen Sun**, Kun Sun, Ning Zhang, and Xu He. "RusTEE: Developing Memory-Safe ARM TrustZone Applications". In: *Proceedings of the 36th Annual Computer Security Applications Conference*. ACSAC '20. Dec. 2020.

[6] Pei Wang, Yu Ding, **Mingshen Sun**, Huibo Wang, Tongxin Li, Rundong Zhou, Zhaofeng Chen, and Yiming Jing. "Building and Maintaining a Third-Party Library Supply Chain for Productive and Secure SGX Enclave Development". In: *The 42nd International Conference on Software Engineering, the Software Engineering In Practice Track*. July 2020.

[7] Yang Hu, **Mingshen Sun**, and John C.S. Lui. "Exploiting Non-Uniform Program Execution Time to Evade Record/Replay Forensic Analysis". In: *Computers & Security* (2019).

[8] Zhuohua Li, Jincheng Wang, **Mingshen Sun**, and John C. S. Lui. "Securing the Device Drivers of Your Embedded Systems: Framework and Prototype". In: *The 3rd International Workshop on Security and Forensics of IoT*. 2019.

[9] Huibo Wang, Pei Wang, Yu Ding, **Mingshen Sun**, Yiming Jing, Ran Duan, Long Li, Yulong Zhang, Tao Wei, and Zhiqiang Lin. "Towards Memory Safety for Enclave Programs with Rust-SGX". In: *The 26th ACM Conference on Computer and Communications Security*. 2019.

[10] **Mingshen Sun**, Xiaolei Li, John C.S. Lui, Richard T.B. Ma, and Zhenkai Liang. "Monet: A User-oriented Behavior-based Malware Variants Detection System for Android". In: *IEEE Transactions on Information Forensics and Security* (2017).

[11] **Mingshen Sun**, Tao Wei, and John C. S. Lui. "TaintART: A Practical Multi-level Information-Flow Tracking System for Android RunTime". In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security*. CCS '16. Vienna, Austria, Oct. 2016.

[12] **Mingshen Sun**, John C. S. Lui, and Yajin Zhou. "Blender: Self-randomizing Address Space Layout for Android Apps". In: *Proceedings of the 19th International Symposium on Research in Attacks, Intrusions and Defenses*. RAID '16. Evry, France, Sept. 2016.

[13] **Mingshen Sun**, Mengmeng Li, and John C. S. Lui. "DroidEagle: Seamless Detection of Visually Similar Android Apps". In: *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '15. New York, USA, June 2015.

[14] **Mingshen Sun**, Min Zheng, John C. S. Lui, and Xuxian Jiang. "Design and Implementation of an Android Host-based Intrusion Prevention System". In: *Proceedings of the 30th Annual Computer Security Applications Conference*. ACSAC '14. New Orleans, USA, Dec. 2014.

[15] Min Zheng, **Mingshen Sun**, and John C. S. Lui. "DroidTrace: A Ptrace Based Android Dynamic Analysis System with Forward Execution Capability". In: *Proceedings of the 10th International Wireless Communications and Mobile Computing Conference*. Nicosia, Cyprus, Aug. 2014.

[16] Min Zheng, **Mingshen Sun**, and John C. S. Lui. "DroidRay: A Security Evaluation System for Customized Android Firmwares". In: *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*. Kyoto, Japan, June 2014.

[17] Min Zheng, **Mingshen Sun**, and John C. S. Lui. "DroidAnalytics: A Signature Based Analytic System to Collect, Extract, Analyze and Associate Android Malware". In: *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. TrustCom '13. Melbourne, Australia, July 2013.

Talks

Feb, 2022 *Proof of Being Forgotten: Verified Privacy Protection in Confidential Computing Platform*, OC3 - Open Confidential Computing Conference 2022, Video

Sept, 2021 *Teaclave: Making Computation on Privacy-Sensitive Data Safe and Simple*, ApacheCon 2021

Aug, 2021 *SGXRay: Automated Vulnerability Finding in SGX Enclave Application*, BlackHat 2021 Arsenal

Aug, 2021 *Apache Teaclave (incubating): Safe and Simple Secure Computing Platform*, ApacheCon Asia 2021

May, 2021 *Apache Teaclave (incubating): An Open Source Universal Secure Computing Platform in Rust*, Cloud Native Rust Day

Mar., 2021 *Teaclave: A Universal Secure Computing Platform*, OC3 - Open Confidential Computing Conference 2021

Sep., 2020 *Teaclave: A Universal Secure Computing Platform*, ApacheCon 2020

Jul., 2020 *Teaclave: A Universal Secure Computing Platform*, SGX Community Day

Sep., 2019 *Rust TrustZone SDK: Enabling Safe, Functional, and Ergonomic Development of Trustlets*, Linaro Connect San Diego 2019, San Diego, USA

Jul., 2019 *Bringing Memory-Safety to Keystone Enclave*, Open-Source Enclaves Workshop (OSEW 2019), Berkeley, USA

Jul., 2019 *A Journey to Mastering Rust*, SJTU GoSSIP @ LoCCS Summer School, Shanghai Jiao Tong University, Shanghai, China

May, 2019 *MesaTEE Village* (co-organized with Yu Ding), DEF CON China 1.0, Beijing, China

Apr., 2019 *Linux From Scratch in Rust*, RustCon Asia 2019, Beijing, China

Apr., 2019 *Build a Secure and Trusted Framework in Rust* (workshop with Yu Ding), RustCon Asia 2019, Beijing, China

Dec., 2018 *Building Safe and Secure Systems in Rust*, RustRush 2018, Moscow, Russia

Oct., 2018 *Building Safe and Secure Systems in Rust: Challenges, Lessons Learned, and Open Questions*, Cybersecurity Speaker Series @ Northeastern Univeristy, Northeastern University, Boston, USA

Jul., 2018 *Rust, Memory-Safety, and Beyond*, SJTU GoSSIP @ LoCCS Summer School, Shanghai Jiao Tong University, Shanghai, China

May, 2018 *When Memory-Safe Languages Become Unsafe*, DEF CON China, Beijing, China

May, 2018 *Towards a Memory-Safe Linux Distribution*, SJTU GoSSIP @ LoCCS, Shanghai Jiao Tong University, Shanghai, China

Dec., 2017 *MesaLock: A Memory-Safe Linux Distribution*, University of Science and Technology of China, Hefei

Nov., 2016 *TaintART: A Practical Multi-level Information-Flow Tracking System for Android RunTime*, GoSSIP @ LoCCS, Shanghai Jiao Tong University, Shanghai

Nov., 2016 Network and Information Security Protection Summit 2016 (XDef 2016), Wuhan

Technical Experience

Extremely Proficient With

language Rust, C/C++, Python, Swift, Java

technology
- System programming, Rust internals, PyPy/RPython internals, trusted execution environment (Intel SGX, ARM TrustZone, and RISC-V Keystone), privacy-preseving computation technologies
- Android OS hacking: frameworks, Dalvik, RunTime (ART), ART compiler, dynamic linker, etc.
- Android app development & reverse engineering: smali, androguard, APIMonitor, etc.
- Malware analysis, detection, and studies on Android OS vulnerabilities

Have Experience With

technology Linux kernel hacking (kernel driver programming), binary analysis, mobile app (Android and iOS) development, web server management, database management, cloud computing (Hadoop), crawler & search engine, and web design & development

other Professional working proficiency in English and native proficiency in Mandarin Chinese

Honors & Awards

Security MSRC 2021 Most Valuable Security Researchers, August, 2021

ACM-ICPC Excellent Award, the 35th ACM-ICPC Asia Regional Contest, Harbin, 2010

Excellent Award, the 4th ACM-ICPC China Northeast Programming Contest, Harbin, 2010

First Prize, the 3rd ACM-ICPC China Liaoning Provincial Programming Contest, Anshan, 2010

Second Prize, the 1st ACM-ICPC China Dalian Metropolitan Provincial Programming Contest, 2010

PROCON International Special Prize, the 21st NAPROCK PROCON Programming Contest (Final), Japan, 2010

scholarship Postgraduate Studentship of CUHK, 2012–2016

Second-class Scholarship of University, 2 %, 2010

First-class Scholarship of University, 1 %, 2009

other Student Travel Grants for ACSAC 2014 [14] and ACM WiSec 2015 [13]

Outstanding Student Leaders and Outstanding Graduates of Liaoning Province

Professional Services

TPC The 1st IEEE International Workshop on Big Data Analytics for Cyber Security and Defence

journal reviewer
IET Information Security
Security and Communication Networks
IEEE Transactions on Dependable and Secure Computing (TDSC)
IEEE Transactions on Mobile Computing (TMC)
IEEE Communications Magazine
IEEE Transactions on Information Forensics and Security (TIFS)
IEEE Transactions on Emerging Topics in Computing

external reviewer
IEEE S&P Workshop on Mobile Security Technologies (MoST) 2016
IEEE Conference on Communications and Network Security (CNS) 2016
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) 2016
ACM Conference on Data and Application Security and Privacy (CODASPY) 2017
IEEE S&P Workshop on Mobile Security Technologies (MoST) 2017
IEEE Symposium on Privacy-Aware Computing (PAC) 2017

Last updated: April 21, 2022