International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2022, 12(3): 259–261, doi: 10.21655/ijsi.1673-7288.00285

Preface

Preface to Special Issue on System Software Security

Min Yang (杨珉)[1], Chao Zhang (张超)[2], Fu Song (宋富)[3], Yuan Zhang (张源)[1]

[1] (School of Computer Science, Fudan University, Shanghai 200438, China)
[2] (Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)
[3] (School of Information Science and Technology, Shanghai Tech University, Shanghai 201210, China)
Corresponding author: Min Yang, m_yang@fudan.edu.cn; Chao Zhang, chaoz@tsinghua.edu.cn;
Fu Song, songfu@shanghaitech.edu.cn; Yuan Zhang, yuanxzhang@fudan.edu.cn

Citation Yang M, Zhang C, Song F, Zhang Y. Preface to special issue on system software security, *International Journal of Software and Informatics*, 2022, 12(3): 259–261. http://www.ijsi.org/1673-7288/285.htm

System software is the fundamental component responsible for controlling and coordinating the hardware and peripherals of computers and supporting the development and operation of applications. It involves a wide range of programs, such as the operating system, compilers, interpreters, databases, runtime environments, and integrated development environments. With the rapid development of artificial intelligence (AI), Internet of Things (IoT), blockchain, system programming languages, cloud computing, open-source instruction sets, and other technologies, a large number of security problems are emerging in system software. Some of the examples include the Meltdown and Spectre attacks that are made possible by CPU speculative execution and software supply chain attacks caused by backdoors and vulnerabilities. Therefore, identifying and mitigating the security risks in system software and defending against those risks play a vital role in ensuring the security of the diversified computer ecosystems.

In recent years, cyberspace security and system software have become a prioritized direction for ensuring national security. Various funding opportunities are provided by governments to support relevant research. Chinese scholars have also made promising progress in this key field, mainly in software security analysis, software vulnerability discovery and exploitation, system security mechanism design, software-hardware co-design mitigations, and so on. These studies have shown two emerging characteristics: One is the fusion of artificial intelligence and interdisciplinary technologies, and the other is the focus of national infrastructure security.

One hot research topic in software security analysis is Binary Code Similarity Analysis (BCSA). In this field, several teams have proposed deep learning-based solutions for applications including similar vulnerability scanning, malware family classification, code plagiarism detection, patch analysis, and reverse engineering assistance. Another one is software supply chain analysis, which aims to identify potential vulnerabilities and other risks by recognizing third-party components. In the field of vulnerability discovery, the community has made significant progress in recent years, by exploring techniques like fuzzing in both depth and breadth. In terms of depth, a number of knowledge- and data-driven solutions and hybrid techniques have been proposed to improve testing efficiency. As for the breadth, specific fuzzing solutions have been designed for different targets, such as open-source user-land software,

Received 2022-06-07; Accepted 2022-06-07; IJSI published online 2022-09-23

kernels, drivers, IoT firmware, virtual machines, network protocols, and blockchains. In the field of vulnerability exploitation, multiple teams addressed several critical challenges in automatic exploitation generation, including automatic heap fengshui, defense passing, and polymorphic payload generation. In the field of system security mechanism design, several new mechanisms have been proposed from the perspectives of isolation, access control, and integrity protection to effectively mitigate zero-day vulnerability attacks. As for the field of software-hardware co-design mitigations, several new features have been proposed and integrated into the CPU to provide software with the support of access control for sensitive operations and integrity protection for stack and kernel objects, which provides better performance and security guarantees. Lastly, Trusted Execution Environment (TEE) solutions (e.g., Penglai) are thoroughly explored to improve system software security.

To timely reflect China's research progress in this field, strengthen the cooperation with overseas researchers interested in system software security, we called for papers for a Special Issue on System Software Security in the *Ruan Jian Xue Bao/Journal of Software* in 2021, selected the best 4 out of the 9 excellent papers from the special issue, and recommended them for bilingual publication in *International Journal of Software and Informatics*. These 4 representative papers are outlined as follows.

By combining model checking and sparse value-flow analysis, the study *Counterexample-guided Spatial Flow Model Checking Methods for C Code* designed a spatial flow model to effectively describe the state behavior of C programs at the symbolic variable level and at the address space level. It also proposed an algorithm of the Counter Example-Guided Abstraction refinement and Sparse value-flow strong update (CEGAS), which enabled points-to-sensitive formal verification of C programs.

To solve two new problems caused by the setup of large secure memory in TEEs, the study *Memory Optimization System for SGXv2 Trusted Execution Environment* put forward a new lightweight code migration approach, which dynamically migrates the code of normal applications into secure memory but leaves the data in place. The migrated code can then use secure memory to avoid the drastic performance degradation caused by disk paging.

Traditional methods for refcount field identification based on code pattern matching have great limitations. For instance, they require expert experience to summarize patterns, which is a laborious job, not to mention that the manually summarized patterns do not cover all cases. To address these issues, the paper *Refcount Field Identification for Linux Kernel Based on Deep Learning* proposed features that can be used to characterize the refcount fields in the kernel, developed a method for refcount field identification based on multimodal deep learning, and tested it empirically on the Linux kernel.

The paper *Exploit-oriented Automated Information Leakage* proposed an Automated Exploit Generation (AEG) solution EoLeak, which uses the analysis of program execution traces to address the challenging AEG problem when protection mechanisms, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), are present in target vulnerable programs.

This Special Issue focuses on the detection, assessment, management, repair, and mitigation of system software defects and vulnerabilities, reflecting the latest research progress of Chinese scholars in related fields. We thank the editorial boards of the *Journal of Software* and *International Journal of Software and Informatics* and the Technical Committee of Systems Software for their guidance and help in the preparation of this special issue. Our gratitude also extends to all the experts on the review panel for their timely, patient, and meticulous review and all the authors for their active contribution. We hope this special issue will help promote the research of system software security.

Min Yang, Ph.D., professor at Fudan University, doctoral supervisor, member of the 8th Cyber Security Discipline Appraisal Group of the Academic Degrees Committee of the State Council, Distinguished Professor of Changjiang Scholars Program of Ministry of Education of China, Chief Scientist of the National 973 Project. He focuses on intelligent system security research, with major progress in malicious code analysis, vulnerability detection, and AI system security. The "Whitzard Team" at Fudan University won great achievements in security competitions under his supervision. He has cultivated a great number of high-level talents for the industry.

Chao Zhang, Ph.D., tenured associate professor at Tsinghua University, CCF senior member, recipient of Tsinghua University Young Faculty Award, MIT TR35 China, and Qiu Shi Outstanding Young Scholar. His main research interests lie in software and system security, especially vulnerability discovery and mitigation. He has published more than 20 papers in the 4 top-tier security conferences. In the Cyber Grand Challenge (CGC) event launched by DARPA, he co-led the Code Jitsu team and achieved great results in the defense.

Fu Song, Ph.D., tenured associate professor and researcher at Shanghai Tech University, doctoral supervisor, selected for Shanghai Pujiang Talent Program, Shanghai Chenguang Scholar, CCF senior member, member of Technical Committee of Formal Methods and Technical Committee of System Software. He has presided and participated in major, key, China-German international cooperation, and general projects of the National Natural Science Foundation of China (NSFC) and has published more than 65 papers. Most of them are published in top journals and conferences in software engineering, such as IEEE TSE, ACM TOSEM, CAV, ICSE, ISSTA, and ASE, and those in system security, such as IEEE S&P and IEEE TDSC. He also won the best paper award of the European Association for Software Science and Technology (EASST). He is mainly engaged in research on the basic theory and applied theory of software and AI security.

Yuan Zhang, Ph.D., associate professor at Fudan University, doctoral supervisor, CCF professional member, selected for Shanghai Rising-Star Program, recipient of ACM SIGSAC China Rising Star Award. His major research interest lies in software security and program analysis, with his works published in top-tier conferences in the area of network and system security and software engineering. He is a Program Committee member of IEEE S&P, USENIX Security, WWW, and other conferences. He is on the Editorial Board of Empirical Software Engineering Journal (EMSE) and acts as a Guest Editor of a Special Issue of *Ruan Jian Xue Bao/Journal of Software*. He has led the team to win the championship of the Innovation & Practice Contest in the National College Student Information Security Contest 2020/2021 and the championship of the National University Cyber Security Association (X-NUCA) Contest 2019/2020.