Dongliang Mu

Associate Professor
School of Cyber Science and Engineering
Huazhong University of Science and Technology
Mingde Building A309, Wuhan, Hubei, China `430043`

dzm91@hust.edu.cn
https://mudongliang.github.io/about
Google Scholar

Research Interests

My current research focuses on Software and System Security. More specifically, my research interests span the areas of Vulnerability Fuzzing, Vulnerability Analysis (including Crash Deduplication, Crash Diagnosis, Vulnerability Reproduction) and Vulnerability Assessment. Currently, I am really interested in the `Vulnerability Fuzzing, Analysis and Fixing` of kernel programs (e.g., Linux Kernel).

Education

14-19 **Ph.D.** in Computer Science and Technology, *Nanjing University*
Adviser: Professor Bing Mao

10-14 **B.E.** in Computer Science and Technology, *Zhengzhou University*

Experiences

08/20-Now **Associate Professor**, *Huazhong University of Science and Technology*

01/20-07/20 **Research Fellow**, *Pennsylvania State University*
Adviser: Professor Xinyu Xing

02/18-03/18 **Organizer of 2018 Penn State Cybersecurity Competition**, *Pennsylvania State University*
HomePage : `https://psusecurity.github.io/`

04/16-12/19 **Research Assistant**, *Pennsylvania State University*
Adviser: Professor Xinyu Xing

09/14-06/16 **Graduate Research and Teaching Assistant**, Nanjing University
Adviser: Professor Bing Mao

Honors & Awards

05/23 **Google Open Source Peer Bonus Award**

02/22 **Wuhan Talent Program**

07/19 **Student Travel Grant of 14th ACM ASIA Conference on Computer and Communications Security**

10/18 **Artificial Intelligence Scholarship at Nanjing University**

10/18 **ACM CCS Outstanding Paper Award (Top 1)**

05/17 **Student Travel Grant of 38th IEEE Symposium on Security and Privacy**

Publications

*** means equal contribution**

Conference Papers:

P-13 **[NDSS 2022] Mu, D.**, Wu, Y., Chen, Y., Lin, Z., Yu, C., Wang, G., Xing, X., An In-depth Analysis of Duplicated Linux Kernel Bug Reports, In Proceedings of the Network and Distributed System Security Symposium, US, February 2022. **(CCF A)**

P-12 **[Oakland SP 2022]** Lin, Z., Chen, Y., **Mu, D.**, Yu, C., Wu, Y., Li, K., Xing, X., GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs, In Proceedings of the 43rd IEEE Symposium on Security and Privacy, Virtual Event, May 2022. **(CCF A)**

P-11

[TrustComm 2021] Chen, L., Guo, J., He, Z., **Mu, D.**, Mao, B., RoBin: Facilitating the Reproduction of Configuration-Related Vulnerability., In Proceedings of the 20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Shenyang, China, October 2021. **(CCF C)**

P-10 **[ASE 2019]** **Mu, D.***, Guo, W.*, Cuevas, A., Chen, Y., Gai, J. Xing, X., Mao, B., Song, C., "RENN: Efficient Reverse Execution with Neural-Network-assisted Alias Analysis", In Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering, San Diego, CA, November 2019. **(CCF A)**

P-9 **[AsiaCCS 2019]** Chen, Y.*, **Mu, D.***, Sun, Z., Xu, J., Shen, W., Xing, X., Lu, L., Mao B., "Ptrix: Efficient Hardware-Assisted Fuzzing for COTS Binary", In Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security, Auckland, New Zealand, July 2019. **(CCF C)**

P-8 **[USENIX Security 2019]** Guo, W.*, **Mu, D.***, Xing, X., Du, M., Song, D., "DEEPVSA: Facilitating Value-set Analysis with Deep Learning for Postmortem Program Analysis", In Proceedings of the 28th USENIX Security Symposium, Santa Clara, California, August 2019. **(CCF A)**

P-7 **[PRICAI 2019]** Guo, W., **Mu, D.**, Chen, L., Gai, J., "Building Adversarial Defense with Non-invertible Data Transformations", In Proceedings of the 16th Pacific Rim International Conference on Artificial Intelligence, Cuvu, Yanuca Island, Fiji, August 2019. **(CCF C)**

P-6 **[CCS 2018]** Guo, W., **Mu, D.**, Xu, J., Su, P., Wang, G., Xing, X., "LEMNA: Explaining Deep Learning based Security Applications", In Proceedings of The 25th ACM Conference on Computer and Communications Security, Toronto, Canada, October 2018. **(CCF A, Outstanding Paper Award)**

P-5 **[USENIX Security 18]** **Mu, D.**, Cuevas, A., Yang, L., Hu, H., Xing, X., Mao, B., Wang, G., "Understanding the Reproducibility of Crowd-reported Security Vulnerabilities", In Proceedings of the 27th USENIX Security Symposium, Baltimore, Mayland, August 2018. **(CCF A)**

P-4 **[SecureCOMM 17]** **Mu, D.**, Guo, J., Ding, W., Wang, Z., Mao, B., Shi, L., "ROPOB: Obfuscating Binary Code via Return Oriented Programming", In International Conference on Security and Privacy in Communication Systems, Niagara Falls, Canada, October 2017. **(CCF C)**

P-3 **[SecureCOMM 17]** Zhu, J., Zhou, W., Wang, Z., **Mu, D.**, Mao, B., "DiffGuard: Obscuring Sensitive Information in Canary Based Protections", In International Conference on Security and Privacy in Communication Systems, Niagara Falls, Canada, October 2017. **(CCF C)**

P-2 **[USENIX Security 17]** Xu, J., **Mu, D.**, Xing, X., Liu, P., Chen, P., Mao, B., "POMP: Postmortem Program Analysis with Hardware-Enhanced Post-Crash Artifacts", In Proceedings of the 26th USENIX Security Symposium, Vancouver, Canada, August 2017. **(CCF A)**

P-1 **[CCS 16]** Xu, J., **Mu, D.**, Chen, P., Wang, P., Xing, X., Liu, P., "CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core Dump", In Proceedings of the 23nd ACM Conference on Computer and Communications Security, Vienna, Austria, October 2016. **(CCF A)**

Journal Papers:

J-1 **[TSE 2019]** **Mu, D.**, Du, Y., Xu, J., Xu, J., Xing, X., Mao, B., "POMP++: Facilitating Postmortem Program Diagnosis with Value-set Analysis", In IEEE Transactions on Software Engineering, 2326-3881, 2019. **(CCF A)**

Academic Service

Reviewer:

[TDSC] IEEE Transactions on Dependable and Secure Computing: Reviewer
[ToSEM] ACM Transactions on Software Engineering and Methodology: Reviewer
[Oakland SP] IEEE Symposium on Security and Privacy: 2021 Subreviewer
[ACM CCS] ACM Conference on Computer and Communications Security: 2019, 2020 Subviewer
[USENIX Security] USENIX Symposium on Security: 2020 Subreviewer
[ACSAC] Annual Computer Security Applications Conference: 2019, 2020 Subviewer
[ISC] Information Security Conference: Reviewer
[JSA] Journal of Systems Architecture: Reviewer

Talks

5/22

Facilitating the Removal of Kernel Vulnerability with Crash Triage
ASSS'22 Workshop, Genoa, Italy

11/21 Towards Facilitating the Removal of Software Vulnerability
Seminar, Qingdao, Shandong, China

11/20 Towards Facilitating the Removal of Software Vulnerability
InforSec Workshop, Wuhan, Hubei, China

7/19 Ptrix: Efficient Hardware-Assisted Fuzzing for COTS Binary
AsiaCCS, Auckland, New Zealand

5/19 Towards Facilitating the Removal of Software Defects
QiZhen Youth Forum in Zhejiang University, Hangzhou, Zhejiang, China

10/18 From Physical Security to Cyber Security: How to forge data spoofing personalized auto insurance
GeekPwn China, Shanghai, China

8/18 Understanding the Reproducibility of Crowd-reported Security Vulnerabilities
USENIX Security, Baltimore, USA

Research Projects

18-19 **Deep Learning Assisted Program Analysis** *Cyber Security Lab, Penn State University*
• Develop deep learning assisted Value Set Analysis to faciliate Postmortem Program Analysis. [See P-7, P-9]

17-18 **Vulnerability Reproduction** *Cyber Security Lab, Penn State University*
• Perform an in-depth analysis on the reproducibility of crowd-reported security vulnerabilities. [See P-5]

16-17 **Analysis on Software Crashes** *Cyber Security Lab, Penn State University*
• Analyze core dumps caused by memory corruption vulnerabilities; locate the crash point; restore the stack trace; narrow down code segments carrying vulnerabilities. [See P-1]
• Enhance a core dump with execution trace logged through Intel Processor Tracing; perform reverse execution and symbolic execution against the trace; pinpoint the root cause of software crash. [See P-2]
• Leverage Value-set Analysis to improve the memory alias problem in the POMP, to achieve better effectiveness and efficiency. [See J-1]

15-16 **Obfuscation based ROP** *System Security Lab, Nanjing University*
• Propose an obfuscation scheme for binaries based on ROP (Return Oriented Programming), which aims to serve as an efficient and deployable anti-reverse-engineering approach. [See P-4]

Teaching

• Software Security, Instructor, Spring 2020, 2021
• Assembling Language, Instructor, Fall 2021

Open Source Projects

06/16 **LinuxFlaw**
• Record all the memory error vulnerabilities we used for our Usenix Security 2018 [see P-5]. We not only disclose the detail of vulnerability reproduction but also try to create docker images about those vulnerabilities as possible as we can.

06/16 **Source-packages**
• Source code for the vulnerable software in the LinuxFlaw

06/16 **Dockerfiles**
• All the useful Dockerfiles and related tools in the LinuxFlaw

05/17 **POMP**
• Leverage Intel PT to do reverse execution, and diagnose the root cause of software failure

06/19 **DEEPVSA**
• Facilitate Value-set Analysis with Recurrent Neural Network for better Postmortem Program Analysis

12/14

Linux-insides

- One book-in-progress about Linux Kernel and its insides.

CVE Discovered

CVE ID	Vulnerability Type	Vulnerable Software	Vulnerable Version
CVE-2018-8816	Stack Exhaustion	perl	5.26.1
CVE-2018-8881	Heap buffer overflow	nasm	2.13.02rc2
CVE-2018-8882	Stack buffer overflow	nasm	2.13.02rc2
CVE-2018-8883	Global buffer overflow	nasm	2.13.02rc2
CVE-2018-10016	Division-by-zero	nasm	2.14rc0
CVE-2018-9138	Stack Exhaustion	binutils	2.29
CVE-2018-9996	Stack Exhaustion	binutils	2.29
CVE-2018-10316	Denial-of-Service	nasm	2.14rc0
CVE-2018-9251	Denial-of-Service	libxml2	2.9.8
CVE-2021-37159	Double Free	Linux Kernel	
CVE-2022-27950	Memory Leak	Linux Kernel	
CVE-2022-30868	Use of Uninitialized Variable	Linux Kernel	
CVE-2022-30869	Improper Input Validation	Linux Kernel	

Upstream Linux Kernel Bug Patches

Age	Kernel Commits
2022-05-17	media: ov7670: remove ov7670_power_off from ov7670_remove
2022-05-13	rtlwifi: Use pr_warn instead of WARN_ONCE
2022-05-06	f2fs: remove WARN_ON in f2fs_is_valid_blkaddr
2022-05-06	HID: bigben: fix slab-out-of-bounds Write in bigben_probe
2022-04-05	tee: optee: add missing mutex_destroy in optee_ffa_probe
2022-03-22	ntfs: add sanity check on allocation size
2022-03-17	fs: erofs: add sanity check for kobject in erofs_unregister_sysfs
2022-03-14	btrfs: don't access possibly stale fs_info data in device_list_add
2022-03-07	media: hdpvr: initialize dev->worker at hdpvr_register_videodev
2022-02-22	media: em28xx: initialize refcount before kref_get
2022-01-24	HID: elo: fix memory leak in elo_probe
2021-12-06	spi: change clk_disable_unprepare to clk_unprepare)
2021-12-03	usb: bdc: fix error handling code in bdc_resume
2021-11-30	dpaa2-eth: destroy workqueue at the end of remove function
2021-11-09	f2fs: fix UAF in f2fs_available_free_memory
2021-10-27	fs: reiserfs: remove useless new_opts in reiserfs_remount
2021-10-25	dmaengine: tegra210-adma: fix pm runtime unbalance in tegra_adma_remove
2021-10-25	dmaengine: tegra210-adma: fix pm runtime unbalance
2021-10-25	dmaengine: rcar-dmac: refactor the error handling code of rcar_dmac_probe
2021-10-24	can: xilinx_can: xcan_remove(): remove redundant netif_napi_del()
2021-10-07	memory: fsl_ifc: fix leak of irq and nand_irq in fsl_ifc_ctrl_probe
2021-09-23	JFS: fix memleak in jfs_mount
2021-08-13	ipack: tpci200: fix memory leak in the tpci200_register
2021-08-13	ipack: tpci200: fix many double free issues in tpci200_pci_probe
2021-08-04	media: em28xx-input: fix refcount bug in em28xx_usb_disconnect
2021-07-22	spi: meson-spicc: fix memory leak in meson_spicc_remove
2021-07-22	media: dvb-usb: Fix error handling in dvb_usb_i2c_init
2021-07-22	media: dvb-usb: fix uninit-value in vp702x_read_mac_addr
2021-07-22	media: dvb-usb: fix uninit-value in dvb_usb_adapter_dvb_init
2021-07-21	usb: hso: remove the bailout parameter
2021-07-21	usb: hso: fix error handling code of hso_create_net_device
2021-07-17	netfilter: nf_tables: fix audit memory leak in nf_tables_commit
2021-07-15	usb: hso: fix error handling code of hso_create_net_device
2021-07-08	ieee802154: hwsim: fix GPF in hwsim_new_edge_nl
2021-07-07	ieee802154: hwsim: fix GPF in hwsim_set_edge_lqi
2021-06-22	ieee802154: hwsim: Fix memory leak in hwsim_add_one
2021-06-18	net: caif: modify the label out_err to out
2021-06-16	net: usb: fix possible use-after-free in smsc75xx_bind
2021-06-14	ieee802154: hwsim: Fix possible memory leak in hwsim_subscribe_all_others
2021-06-08	media: dvd_usb: memory leak in cinergyt2_fe_attach
2021-06-02	ALSA: control led: fix memory leak in snd_ctl_led_register
2021-05-21	misc/uss720: fix memory leak in uss720_probe
2021-05-17	NFC: nci: fix memory leak in nci_allocate_device
2021-01-26	usbnet: fix the indentation of one code snippet
2018-08-08	scsi: aacraid: Spelling fix in comment