

# Dongliang Mu

---

WestGate Building E343  
The Pennsylvania State University  
State College, PA 16802

814-880-8328  
[mudongliangabcd@outlook.com](mailto:mudongliangabcd@outlook.com)  
<https://mudongliang.github.io/about>

## Research Interests

My current research focuses on **Software Security and System Security**. More specifically, my research interests span the areas of Vulnerability Reproduction, Postmortem Program Analysis, Vulnerability Diagnosis, and Binary Analysis.

## Education

- 2014-2020 **Ph.D. Candidate** in Software Security, *Nanjing University*  
Adviser: [Prof. Bing Mao](#)
- 2010-2014 **B.E** in Computer Science and Technology, *Zhengzhou University*

## Experiences

- 10/2018 Talk in the GeekPwn China  
From Physical Security to Cyber Security: How to forge data spoofing personalized auto insurance
- 02/2018 **Organizer** of 2018 Penn State Cybersecurity Competition in *Pennsylvania State University*  
HomePage : <https://psusecurity.github.io/>
- 2016-Now **Research Assistant** in *Pennsylvania State University*  
Adviser: [Prof. Xinyu Xing](#)

## Publications

- P-10 **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 (TSE), **Accepted**.
- P-9 **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 (ASE 2019), San Diego, CA, November 2019.
- P-8 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(AsiaCCS 2019), Auckland, New Zealand, July 2019.
- P-7 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 (USENIX Security 2019), Santa Clara, California, August 2019.
- P-6 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 (CCS 2018), Toronto, Canada, October 2018. **(Outstanding Paper Award)**
- P-5 **Mu, D.**, Cuevas, A., Yang, L., Hu, H., Wang, G., Xing, X., Mao, B., “Understanding the Reproducibility of Crowd-reported Security Vulnerabilities”, In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, Maryland, August 2018.
- P-4 **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 (SecureCOMM 17), Niagara Falls, Canada, October 2017.
- P-3 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 (SecureCOMM 17), Niagara Falls, Canada, October 2017.
- P-2 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 (USENIX Security 17), Vancouver, Canada, August 2017.

- P-1 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 23rd ACM Conference on Computer and Communications Security (CCS 16), Vienna, Austria, October 2016.  
Note that, \* means equal contribution.

## Research Projects

- 2018-2019 **Deep Learning Assisted Program Analysis** *Cyber Security Lab, Penn State University*  
• develop deep learning assisted Value Set Analysis to facilitate Postmortem Program Analysis. [See P-7, P-9]
- 2017-2018 **Vulnerability Reproduction** *Cyber Security Lab, Penn State University*  
• perform the in-depth analysis on the reproducibility of crowd-reported security vulnerabilities. [See P-5]
- 2016-2017 **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 P-10]
- 2015-2016 **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]

## Honors & Awards

- 07/2019 **Student Travel Grant of 14th ACM ASIA Conference on Computer and Communications Security**
- 10/2018 **Artificial Intelligence Scholarship in Nanjing University**
- 05/2017 **Student Travel Grant of 38th IEEE Symposium on Security and Privacy**

## Open Source Projects

- 06/2016 **[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.
- 06/2016 **[Source-packages](#)**  
• Source code for the vulnerable software in the LinuxFlaw
- 06/2016 **[Dockerfiles](#)**  
• All the useful Dockerfiles and related tools in the LinuxFlaw
- 04/2016 **[TraditionalMitigation](#)**  
• Summarize traditional mitigations in GCC to defend Memory Corruption Vulnerability
- 05/2017 **[POMP](#)**  
• Leverage Intel PT to do reverse execution, and diagnose the root cause of software failure
- 06/2019 **[DEEPVSA](#)**  
• Facilitate Value-set Analysis with Recurrent Neural Network for better Postmortem Program Analysis

## Books In Progress

- 12/2014 **[Linux-insides](#)**  
• One book-in-progress about Linux Kernel and its insides.
- 12/2014 **[Linux-insides-zh](#)**  
• Chinese Translation of [linux-insides](#). This upstream repo is a 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

Last updated: October 18, 2019

[Dongliang Mu de Blog](#)