Xinyu Xing

Contact Information

Department of Computer Science
Northwestern University, IL, US

xinyu.xing@northwestern.edu
http://xinyuxing.org/

Research Interests

My research endeavors lie primarily in the area of software, system, and AI Security.

Education

Georgia Institute of Technology, US
Ph.D. / Computer Science
Advisors: Wenke Lee and Nick Feamster *2011 - 2015*

Honors and Awards

CSAW Best Applied Research Paper Award (*the top 10 Finalists*) (2023)
Winner of Pwn2Own (2022)
Amazon Research Award (2022)
NSF CAREER Award (2021)
Amazon Research Award (2020)
IST Junior Faculty Excellence in Research Award (2020)
2 IBM Research Fellowship (Wenbo Guo & Yueqi Chen) (2020)
The BlackHat highly-anticipated talk (BlackHat Europe 2019)
The Outstanding Paper Award of the 25th ACM Conference on Computer and Communications Security (CCS 2018)
GeekPwn Hall of Fame (Shanghai, 2018)
DEF CON/GeekPwn Competition on Adversarial Attacks and Defenses with team JD-Omega (*the top 6 Finalists*) (CAAD, Las Vegas, 2018)
GeekPwn on AI Data Tracking Challenge with team JD-Omega (*the 9th place*) (DT, Beijing, 2018)
The Best Paper Award of Annual Computer Security Applications Conference (ACSAC 2017)
CSAW Best Applied Research Paper Award (*the top 10 Finalists*) (2016)
Google Security Hall of Fame (2013)

Work Experience

Associate Professor, (Northwestern University, Evanston, US) *Sep. 2021 - present*

Co-founder, (Sec3, Texas, US) *Nov. 2022 - present*

Assistant Professor, (Pennsylvania State University, State College, US) *Aug. 2015 - 2021. Dec.*

Graduate Research Assistant, (Georgia Institute of Technology, Atlanta, US)
Advisors: Wenke Lee and Nick Feamster *Aug. 2011 - Aug. 2015*

Research Intern, (Microsoft Research, Redmond, US)
Mentors: Helen Wang *May - Jul. 2013*

Research Intern, (Microsoft Research, Redmond, US)
Mentors: Himanshu Raj *Jun. - Aug. 2012*

Graduate Research Assistant, (University of Colorado, Boulder, US)
Advisors: Richard Han and Shivakant Mishra *Jan. 2009 - Jun. 2011*

Publications

* **indicates the student or postdoc I advised.**

[C.70] Lin, Z.*, Yu, Z.*, Guo, Z.*, Campanoni, S., Dinda, P., Xing, X., "CAMP: Compiler and Allocator-based Heap Memory Protection", *Proceedings of the 33rd USENIX Security Symposium (USENIX Security)*. Philadelphia, 2024.

[C.69] Cheng, Z.*, Wu, X.*, Yu, J.*, Sun, W., Guo, W., Xing, X., "StateMask: Explaining Deep Reinforcement Learning through State Mask", *Proceedings of the 37th Annual Conference on Neural Information Processing Systems (NeurIPS)*. New Orleans, 2023.

[C.68] Lin, Z.*, Xing, X., Chen, Z., Li, K., "ad io_uring: A New Era of Rooting for Android", *Blackhat USA*. Las Vegas, 2023.

[C.67] Zeng, K., Lin, Z.*, Lu, K., Xing, X., Wang, R., Doupe, A., Shoshitaishvili, Y., Bao, T., "RetSpill: Igniting User-Controlled Data to Burn Away Linux Kernel Protections", *Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS)*. Copenhagen, 2023.

[C.66] Wu,Y.*, Lin, Z.*, Chen, Y., Le, D.*, Mu, D., Xing, X.,,"Mitigating Security Risks in Linux with KLAUS : A Method for Evaluating Patch Correctness", Proceedings of the 32nd USENIX Security Symposium (USENIX Security), Anaheim, August 2023.

[C.65] Guo, W., Wu, X., Wang, L., Song, D., Xing, X.,,"PATROL: Provable Defense against Adversarial Policy in Two-player Games", Proceedings of the 32nd USENIX Security Symposium (USENIX Security), Anaheim, August 2023.

[C.64] Wu, X.*, Guo, W., Yan, J.*, Coskun, B., Xing, X., "From Grim Reality to Practical Solution: Malware Classification in Real-World Noise", Proceedings of the 44th IEEE Symposium on Security and Privacy (IEEE S&P), San Francisco, May 2023.

[C.63] Yu, J.*, Guo, W., Qin, Q.*, Wang, G., Wang, T., Xing, X., "AIRS: Explanation for Deep Reinforcement Learning based Security Applications", *Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*. Anaheim, 2023.

[C.62] Lin, Z.*, Wu, Y.*, Xing, X., "Cautious! A New Exploitation Method! No Pipe but as Nasty as Dirty Pipe", *Blackhat USA*. Las Vegas, 2022.

[C.61] Qin, Q., JiYang, J., Song, F., Chen, T., Xing, X., "DeJITLeak: Eliminating JIT-Induced Timing Side-Channel Leaks", *Proceedings of the ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE)*. Singapore, 2022.

[C.60] Lin, Z.*, Wu, Y.*, Xing, X., "DirtyCred: Escalating Privilege in Linux Kernel", *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)*. Los Angeles, 2022.

[C.59] Zeng, K., Chen, Y.*, Cho, H., Xing, X., Doup, A., Bao, T., Yan, S., "Playing for K(H)eaps: Understanding and Improving Linux Kernel Exploit Reliability", *Proceedings of the 31st USENIX Security Symposium (USENIX Security)*. Boston, 2022.

[C.58] Mu, D.*, Wu, Y.*, Chen, Y.*, Lin, Z.*, Xing, X., "An In-depth Analysis of Duplicated Linux Kernel Bug Reports", *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. San Diego, 2022.

[C.57] Lin, Z.*, Wu, Y.*, Chen, Y.*, Mu, D., Li, K., Xing, X., "GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs", *Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P)*. San Francisco, 2022.

[C.56] Guo, W.*, Wu, X.*, Khan, U., Xing, X., "EDGE: Explaining Deep Reinforcement Learning Policies", *Proceedings of The 35th Annual Conference on Neural Information Processing Systems (NeurIPS)*. Virtual event, 2021.

[C.55] Guo, W.*, Wu, X.*, Huang, S., Xing, X., "Adversarial Policy Learning in Two-party Competitive Games", *Proceedings of The 38th International Conference on Machine Learning (ICML)*. Virtual event, 2021.

[C.54] Lu, Y., Guo, W.*,, Xing, X., Noble, W., "DANCE: Enhancing saliency maps using decoys", *Proceedings of The 38th International Conference on Machine Learning (ICML)*. Virtual event, 2021.

[C.53] Xie, X., Guo, W.*, Ma, L., Le, W., Wang, J., Zhou, L., Liu, Y., Xing, X., "Automatic RNN Repair via Model-based Analysis", *Proceedings of The 38th International Conference on Machine Learning (ICML)*. Virtual event, 2021.

[C.52] Wang. L., Javed, Z., Wu, X.*, Guo, W.*, Xing, X., Song, D., "BACKDOORL: Backdoor Attack against Competitive Reinforcement Learning", *Proceedings of The 30th International Joint Conference on Artificial Intelligence (IJCAI)*. Virtual event, 2021.

[C.51] Dai, J., Zhang, Y., Xu, H., Lyu, H., Wu, Z., Xing, X., Yang, M., "Facilitating Vulnerability Assessment through PoC Migration", *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS)*. Virtual event, 2021.

[C.50] Chen, Y.*, Lin, Z.*, Xing, X., "A General Approach to Bypassing Many Kernel Protections and its Mitigation", *Blackhat Asia*. Singapore, 2021.

[C.49] Liang, J.*, Guo, W.*, Luo, T., Honavar, V., Wang, G., Xing, X., "FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data", *Proceedings of The Network and Distributed System Security Symposium (NDSS)*. Virtual, 2021.

[C.48] Yang, L., Guo, W.*, Hao, Q., Ciptadi, A., Ahmadzadeh, A., Xing, X., Wang, G., "CADE: Detecting and Explaining Concept Drift Samples for Security Applications", *Proceedings of the 30th USENIX Security Symposium (USENIX Security)*. Vancouver, Canada, 2021.

[C.47] Wu, X.*, Guo, W.*, Wei, H.*, Xing, X., "Adversarial Policy Training against Deep Reinforcement Learning", *Proceedings of the 30th USENIX Security Symposium (USENIX Security)*. Vancouver, Canada, 2021.

[C.46] Guo, W.*, Wang, L., Xu, Y.*, Xing, X., Du, M., Song, D. "TABOR: A Highly Accurate Approach to Inspecting and Restoring Trojan Backdoors in AI Systems", *Proceedings of the IEEE International Conference on Data Mining (ICDM)*. Sorrento, Italy, 2020. (Oral Presentation)

[C.45] Chen, Y.*, Lin, Z.*, Xing, X., "A Systematic Study of Elastic Objects in Kernel Exploitation", *Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS)*. Orlando, USA, 2020.

[C.44] Ying, K., Luo, T., Xing, X., Su, J.,, "Superman Powered by Kryptonite: Turn the Adversarial Attack into Your Defense Weapon", *Blackhat USA*. Las Vegas, USA, 2020.

[C.43] Guo, W.*, Wu, X.*, Xing, X., Su, J., "Ruling StarCraft Game Spitefully – Exploiting the Blind Spot of AI-Powered Game Bots", *Blackhat USA*. Las Vegas, USA, 2020.

[C.42] Z. Jiang, Y. Zhang, J. Xu, Q. Wen, Z. Wang, X. Zhang, X. Xing, M. Yang, Z. Yang "PDiff: Semantic-based Patch Presence Testing for Downstream Kernels", *Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS))*. Orlando, USA, 2020.

[C.41] Dai, J., Jiang, Z., Zhang, Y., Zhou, Y., Chen, J, Zhang, X., Tan, X., Yang, M., Xing, X., "BScout: Direct Whole Patch Presence Test for Java Executables", *Proceedings of the 29th USENIX Security Symposium (USENIX Security)*. Boston, USA, 2020.

[C.40] Chen, Y.*, Xing, X., Su, J., "Hands Off and Putting SLAB/SLUB Feng Shui in a Blackbox", *Blackhat Europe*. London, UK, 2019.

[C.39] Chen, Y.*, Xing, X., "SLAKE: Facilitating Slab Manipulation for Exploiting Vulnerabilities in the Linux Kernel", *Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS)*. London, UK, 2019.

[C.38] Liu, F., Wen, Y., Zhang, D., Jiang, X., Xing, X., Meng, D., "Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise", *Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS)*. London, UK, 2019.

[C.37] Mu, D.*, Guo, W.*, Chen, Y.*, Cuevas, A.*, Xing, X., Bing, M, Song, C., "RENN: Efficient Reverse Execution with Neural-Network-assisted Alias Analysis", *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. San Diego, US, 2019.

[C.36] Chen, Y., Mu, D.*, Xu, J.*, Sun, Z., Shen, W., Xing, X., Lu, L., Mao, B., "Ptrix: Efficient Hardware-Assisted Fuzzing for COTS Binary", *Proceedings of the 14th ACM Asia Conference on Information, Computer and Communications Security (AsiaCCS)*. Auckland, New Zealand, 2019.

[C.35] Alrizah, M.*, Zhu, S., Xing, X., Wang, G., "Errors, Misunderstandings, and Vulnerabilities: Analyzing the Crowdsourcing Process of Ad-blocking Systems", *Proceedings of the ACM Internet Measurement Conference (IMC)*. Amsterdam, Netherlands, 2019.

[C.34] Wu, W.*, Chen, Y.*, Xing, X., Zou, W., "KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities", *Proceedings of the 28th USENIX Security Symposium (USENIX Security)*. Santa Clara, USA, 2019.

[C.33] Guo, W.*, Mu, D.*, Xing, X., Du, M., Song, D., "DEEPVSA: Facilitating Value-set Analysis with Deep Learning for Postmortem Program Analysis", *Proceedings of the 28th USENIX Security Symposium (USENIX Security)*. Santa Clara, USA, 2019.

[C.32] Dong, Y.*, Guo, W.*, Chen, Y.*, Xing, X., Zhang, Y., Wang, G., "Towards the Detection of Inconsistencies in Public Security Vulnerability Reports", *Proceedings of the 28th USENIX Security Symposium (USENIX Security)*. Santa Clara, USA, 2019.

[C.31] Zhang, M., Meng, W., Lee, S., Lee, B., Xing, X., "All Your Clicks Belong to Me: Investigating Click Interception on the Web", *Proceedings of the 28th USENIX Security Symposium (USENIX Security)*. Santa Clara, USA, 2019.

[C.30] Guo, W.*, Huang, S., Tao, Y., Xing, X., Lin, L., "Explaining Deep Learning Models – A Bayesian Non-parametric Approach", *Proceedings of the 32nd Annual Conference on Neural Information Processing Systems (Neurips)*. Montreal, Canada, 2018.

[C.29] Guo, W.*, Wang, Q.*, Zhang, K.*, Huang, S., Giles, L., Liu, X., Lin, L., Xing, X., "Defending against Adversarial Samples without Security through Obscurity", *Proceedings of the IEEE International Conference on Data Mining (ICDM)*. Singapore, 2018.

[C.28] Wu, W.*, Xing, X., Su, J., "From Thousands of Hours to a Couple of Minutes: Automating Exploit Generation for Arbitrary Types of Kernel Vulnerabilities", *Blackhat USA*. Las Vegas, US, 2018.

[C.27] Guo, W.*, Mu, D.*, Xu, J.*, Su, P., Wang, G., Xing, X., "LEMNA: Explaining Deep Learning based Security Applications", *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS)*. Toronto, Canada, 2018.

[C.26] Wu, W.*, Chen, Y.*, Xu, J.*, Xing, X., Zou, W., "Towards Facilitating Exploit Generation for Kernel Use-After-Free Vulnerabilities", *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. Baltimore, USA, 2018.

[C.25] Mu, D.*, Villalba, A.*, Yang, L., Hu, H., Wang, G., Xing, X., Mao, B., "Understanding and Measure Reproducibility of Crowd-reported Security Vulnerabilities", *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. Baltimore, USA, 2018.

[C.24] Huang, J., Xu, J.*, Xing, X., Liu, P., Qureshi, M., "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware", *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*. Dallas, USA, 2017.

[C.23] Xu, J.*, Mu, D.*, Xing, X., Liu, P., Mao, B., Chen, P., "POMP: Postmortem Program Analysis with Hardware-Enhanced Post-Crash Artifacts", *Proceedings of the 26th USENIX Security Symposium (USENIX Security)*. Vancouver, Canada, 2017.

[C.22] Wang, Q.*, Guo, W.*, Zhang, K.*, Ororbia, A., Xing, X., Liu, X., Giles, C., "Adversary Resistant Deep Neural Networks with an Application to Malware Detection", *Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*. Halifax, Canada, 2017.

[C.21] Luo, L., Zeng, Q., Cao, C., Chen, K., Liu, J., Liu, L., Gao, N., Yang, M., Xing, X., Liu, P., "System Service Call-oriented Symbolic Execution of Android Framework with Applications to Vulnerability Discovery and Exploit Generation", *Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*. Niagara Falls, US, 2017.

[C.20] Guan, L.*, Liu, P., Xing, X., Ge, X., Zhang, S., Yu, M., Jaeger, T., "TrustShadow: Secure execution of unmodified applications with ARM TrustZone", *Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*. Niagara Falls, US, 2017.

[C.19] Guan, L.*, Jia, S., Chen, B., Zhang, Z., Luo, B., Lin, J., Liu, L., Xing, X., and Xia, L., "Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices", *Proceedings of the 33rd Annual Conference on Computer Security Applications (ACSAC)*. Orlando, US, December 2017.

[C.18] Chen, P.*, Xu, J.*, Hu, Z., Xing, X., Zhu, M., Mao, B., Liu, P., "What You See is Not What You Get! Thwarting Just-in-Time ROP with Chameleon", *Proceedings of the 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Denver, US, June 2017.

[C.17] Xu, J.*, Mu, D.*, Chen, P., Xing, X., Liu, P., "CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core Dump", *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*. Vienna, Austria, 2016.

[C.16] Guan, L.*, Xu, J.*, Wang, S., Xing, X., Lin, L., Huang, H., Liu, P., Lee, W., "From Physical to Cyber: Escalating Protection for Personalized Auto Insurance", *Proceedings of the 14th ACM Conference on Embedded Networked Sensor Systems (Sensys)*. Palo Alto, US, 2016.

[C.15] Wang, W., Zheng, Y., Xing, X., Kwon, Y., Zhang, X., Eugster, P., "WebRanz: Web Page Randomization For Better Advertisement Delivery and Web-Bot Prevention", *Proceedings of the 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE)*. Seattle, US, 2016.

[C.14] Meng, W., Lee, B., Xing, X., Lee, W., "TrackMeOrNot: Enabling Flexible Control on Web Tracking", *Proceedings of the 25th International World Wide Web Conference (WWW)*. Montreal, Canada, 2016.

[C.13] Xu, M., Jang, Y., Xing, X. , Kim, T., Lee, W., "UCognito: Private Browsing without Tears", *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, US, October 2015.

[C.12] Xing, X., Meng, W., Lee, B., Weinsberg, U., Perdisci, R., Sheth, A., Lee, W., "Understanding Malvertising Through Ad-Injecting Browser Extensions", *Proceedings of the 24th International World Wide Web Conference (WWW)*. Florence, Italy, 2015.

[C.11] Meng, W., Xing, X., Sheth, A., Weinsberg, U., Lee, W., "Your Online Interests - Pwned! A Pollution Attack Against Targeted Advertising", *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*. Scottsdale, Arizona, US, 2014.

[C.10] Xing, X., Meng, W., Doozan, D., Feamster, N., Lee, W., Snoeren, A., "Exposing Inconsistent Web Search Results with Bobble", *Proceedings of the 2014 Passive and Active Measurement Conference (PAM)*. Los Angeles, CA, US, 2014.

[C.9] Xing, X., "Depersonalize Search Results with Bobble", *Blackhat Europe*. Amsterdam, Netherlands, 2013.

[C.8] Xing, X., Meng, W., Doozan, D., Snoeren, A., Feamster, N., Lee, W., "Take This Personally: Pollution Attacks on Personalized Services", *Proceedings of the 22nd USENIX Security Symposium (USENIX Security)*, Washington DC, US, 2013.

[C.7] Xing, X., Liang, Y., Huang, S., Cheng, H., Han, R., Lv, Q., Liu, X., Mishra, S., Zhu, Y., "Scalable Misbehavior Detection in Online Video Chat Services", *Proceedings of the 18th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*, Beijing, CHN, 2012.

[C.6] Cheng, H., Liang, Y., Xing, X., Liu, X., Han, R., Lv, Q., Mishra, S., "FGC: Fine-Grained Cascaded Classification for Efficient Misbehaving User Detection in Online Video Chat Services", *Proceedings of the 5th ACM International Conference on Web Search and Data Mining (WSDM)*, Seattle, US, 2012.

[C.5] Xing, X., Liang, Y., Cheng, H., Dang, J., Han, R., Liu, X., Lv, Q., Mishra, S., "SafeVchat: Detecting Obscene Content and Misbehaving Users in Online Video Chat Services", *Proceedings of the 20th International World Wide Web Conference (WWW)*, Hyderabad, IND, 2011.

[C.4] Xing, X., Dang, J., Mishra, S., Liu, X., "A Highly Scalable Bandwidth Estimation of Commercial Hotspot Access Points", *Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM)*, Shanghai, CHN, 2011.

[C.3] Xing, X., Gartrell, M., Beach, A., Han, R., Lv, Q., Mishra, S., Saeda, K., "Enhancing Group Recommendation by Incorporating Social Relationship Interactions", *Proceedings of the 2010 International ACM SIGGROUP conference on Supporting Group Work (SIGGROUP)*, Sanibel Island, US, 2010.

[C.2] Xing, X., Mishra, S., Liu, X., "ARBOR: Hang Together rather than Hang Separately in 802.11 WiFi Networks", *Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM)*, San Diego, US, 2010.

[C.1] Beach, A., Gartrell, M., Xing, X., Han, R., Lv, Q., Mishra, S., Saeda, K., "Fusing Mobile, Sensor and Social Data to Fully Enable Context-Aware Computing", *Proceedings of the 11th ACM Workshop on Mobile Computing Systems and Applications (HOTMOBILE)*, Annapolis, US, 2010.

[J.6] Mu, D.*, Xu, J.*, Xing, X., Liu, P., Mao, B., Chen, P., "POMP++: Facilitating Postmortem Program Diagnosis with Value-set Analysis", *Transactions on Software Engineering (TSE), 2019.*

[J.5] Luo, L., Zeng, Q., Cao, C., Chen, K., Liu, J., Liu, L., Gao, N., Yang, M., Xing, X., Liu, P., "Tainting-Assisted and Context-Migrated Symbolic Execution of Android Framework for Vulnerability Discovery and Exploit Generation", *IEEE Transactions on Mobile Computing (TMC), 2019.*

[J.4] Guan, L.*, Cao, C., Liu, P., Xing, X., Ge, X., Zhang, S., Yu, M., Jaeger, T., "Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM", *IEEE Transactions on Dependable and Secure Computing (TDSC), 2018.*

[J.3] Wang, Q.*, Zhang, K.*, Ororbia, A., Xing, X., Liu, X., Giles, L., "An Empirical Evaluation of Recurrent Neural Network Rule Extraction", *Neural Computation (NECO), 2018.*

[J.2] Cheng, H., Xing, X., Liu, X., Lv, Q., "ISC: an Iterative Social based Classifier for Adult Account Detection on Twitter", *IEEE Transactions on Knowledge and Data Engineering (TKDE), 2014.*

[J.1] Xing, X., Liang, Y., Cheng, H., Dang, J., Han, R., Liu, X., Lv, Q., Mishra, S., "SafeVchat: A System for Obscene Content Detection in Online Video Chat Services", *ACM Transactions on Internet Technology (TOIT), Volume 12, Issue 4, Jul. 2013.*

Research Funding and Gift

DARPA, "Analysis and Restructuring for Containment (ARC)", (Recommended to award)

DARPA, "Euryale: Combating Emergent Execution with a GLANCE", (accumulative fund, Co-PI, Oct. 2022 – Aug. 2026).

Amazon, "Battling Noisy-label Classification", ($100,000, Sole PI, Sep. 2022 – Aug. 2023).

NSF, "Collaborative Research: SaTC: CORE: Small: Towards Label Enrichment and Refinement to Harden Learning-based Security Defenses", ($500,000, Co-PI, Oct. 2021 – Sep. 2024)(My share: $250,000).

NSF, "CAREER: Securing Deep Reinforcement Learning", ($550,000, Sole PI, Sep. 2021 – Aug. 2026).

NSF, "SaTC: CORE: Small: Collaborative: Towards Facilitating Kernel Vulnerability Reproduction by Fusing Crowd and Machine Generated Data", ($500,000, Lead PI, Sep. 2020 – Aug. 2023) (My share: $320,000).

Amazon, "Fine-grained Malware Classification using Coarse-grained Labels", ($90,000, Sole PI, Sep. 2020 – Aug. 2021).

ONR, "Towards the exploitability escalation for software vulnerabilities", ($450,000, Sole PI, Jan. 2020 – Dec. 2022).

NSF, "SaTC: CORE: Small: Towards Locating Memory Corruption Vulnerabilities from Memory Dumps", ($500,000, Sole PI, Aug. 2017 – Jul. 2020)

NSA, "A cyber competition on crash forensics against memory corruption attacks", ($14,500, Co-PI with Peng Liu and Nicklaus Giacobe, Sep. 2016 – Aug. 2017).

"NVIDIA Hardware Grant", (about $8,000, Sole PI, Mar. 2016 / 2017).

Penn State Seed Funding, "Adversary Resistant Deep Neural Networks for Malware Detection", (2 RAs – about $80,000, Sole PI, Sep. 2016 – Aug. 2017).

Penn State ICS Awards Seed Funding Initiative Grants, "From Physical to Cyber: Escalating Protection for Internet of Me", (1 RA – about $40,000, Sole PI, Jan. 2016 – Dec. 2016).

Media Coverage

"DirtyCred Vulnerability Haunting Linux Kernel for 8 Years", SecurityWeek.

"How hackers use tricks to make money from your clicks", NewScientist.

"AI for Security", China Daily (in Chinese).

"Four Cool Tools Expected Out of Black Hat", Security Boulevard.

"Automating Kernel Exploitation for Better Flaw Remediation", Dark Reading.

"Private Browsing: Do Chrome and Firefox Reveal Users? Weird Interests?", Observer Innovation.

"Bye bye, unwanted flesh on Chatroulette", NewScientist.

"Flasher Detection Algorithm Aims to Clean Up Video Chat", MIT Technology Review.

"Researchers Find Privacy Flaws in Chatroulette", New York Times.

Software Data Release

GREBE

`https://github.com/markakd/GREBE`

DirtyCred

https://github.com/markakd/DirtyCred

EDGE
https://github.com/Henrygwb/edge

ELOISE
https://github.com/chenyueqi/w2l

SLAKE
https://github.com/chenyueqi/SLAKE

VIEM
https://github.com/pinkymm/inconsistency_detection

Explainable AI Project
https://github.com/Henrygwb/Explaining-DL

DEEPVSA
https://github.com/Henrygwb/deepvsa

KEPLER
https://github.com/ww9210/kepler-cfhp

FUZE
https://github.com/ww9210/Linux_kernel_exploits

300+ Reproducible CVEs
https://vulnreproduction.github.io/

POMP
https://github.com/junxzm1990/pomp

Teaching Experience

Lecturer, (Northwestern University, Evanson, US)
Undergraduate course: Introduction to Computer Security (COMP_SCI 350)
Overall rating: 5.0/6.0 *Fall 23*

Lecturer, (Northwestern University, Evanson, US)
Undergraduate course: Advanced Offense and Defense in Cybersecurity (COMP_SCI 396)
Overall rating: 6.0/6.0 *Fall 23*

Lecturer, (Northwestern University, Evanson, US)
Graduate course: Advanced System Security (COMP_SCI 496)
Overall rating: 5.5/6.0 *Spring 23*
Overall rating: 5.7/6.0 *Spring 22*

Lecturer, (Pennsylvania State University, University Park, US)
Undergraduate course: Cybersecurity Analytics (IST 820) *Fall 20*

Lecturer, (Pennsylvania State University, University Park, US)
Undergraduate course: Malware Analytics (CYBER 366) *Fall 19, Spring 21*

Lecturer, (Pennsylvania State University, University Park, US)
Graduate course: Software Security (IST 543) *Spring 19*

Lecturer, (Pennsylvania State University, University Park, US)
Undergraduate course: Overview of Information Security (SRA 221) *Fall 15/17/18, Spring 16/21*

Lecturer, (Pennsylvania State University, University Park, US)
Undergraduate course: Network Security (IST 451) *Spring 17*

Teaching Assistant, (Georgia Institute of Technology, Atlanta, US)
Graduate course: Introduction to Information Security (CS-6035) *Fall 14*

Teaching Assistant, (Georgia Institute of Technology, Atlanta, US)
Undergraduate course: Introduction to Information Security (CS-4235) *Fall 12*

Advising

PHD student, (Northwestern University, Evanston, US)
Ziyi Guo (Co-advise with Dr. Yan Chen) *Aug. 2023 - present*

PHD student, (Northwestern University, Evanston, US)
Dang Le *Aug. 2023 - present*

PHD student, (Northwestern University, Evanston, US)
Xinqian Sun *Aug. 2023 - present*

PHD student, (Northwestern University, Evanston, US)
Zelei Cheng *Aug. 2023 - present*

PHD student, (Northwestern University, Evanston, US)
Wenxuan Shi *Aug. 2022 - present*

PHD student, (Northwestern University, Evanston, US)
Zheng Yu *Aug. 2022 - present*

PHD student, (Northwestern University, Evanston, US)
Yuhang Wu *Aug. 2021 - present*

PHD student, (Northwestern University, Evanston, US)
Jiahao Yu *Aug. 2021 - present*

PHD student, (Northwestern University, Evanston, US)
Xian Wu *Aug. 2019 - present*

PHD student, (Northwestern University, Evanston, US)
Zhenpeng Lin
Job: *Researcher Scientist, Apple Inc.* *Aug. 2019 - Aug. 2023*

PHD student, (Pennsylvania State University, University Park, US)
Wenbo Guo
Job: *Assistant Professor, CS Dept, Purdue University* *Aug. 2017 - Aug. 2022*

PHD student, (Pennsylvania State University, University Park, US)
Yueqi Chen
Job: *Assistant Professor, CS Dept., University of Colorado – Boulder* *Aug. 2017 - Aug. 2022*

PHD student, (Pennsylvania State University, University Park, US)
Jun Xu (co-advise with Dr. Peng Liu)

Job: *Assistant Professor, CS Dept., University of Utah* *Aug. 2015 - Aug. 2018*

Postdoc, (Pennsylvania State University, University Park, US)
Le Guan (co-advise with Dr. Peng Liu)

Job: *Assistant Professor, CS Dept., University of Georgia* *Aug. 2015 - Aug. 2018*

Visiting PHD student, (Nanjing University, China)
Dongliang Mu

Job: *Associate Professor, Huazhong University of Science and Technology (HUST)* *Mar. 2016 - Jul. 2020*

Visiting PHD student, (Chinese Academy of Sciences, China)
Wei Wu

Job: *Research Scientist, Huawei Technologies Co., Ltd.* *Aug. 2017 - Nov. 2018*

Visiting PHD student, (McGill University, Canada)
Qinglong Wang

Job: *Assistant Professor, Zhejiang University* *Jul. 2016 - Nov. 2017*

Academic Service

Panel for National Science Foundation SaTC 2023

Panel for National Science Foundation SaTC-TTP 2020

Panel for National Science Foundation SaTC-EDU 2016

Dissertation committee for Wenbo Guo (Pennsylvania State University) 2019

Dissertation committee for Yueqi Chen (Pennsylvania State University) 2020

Dissertation committee for Jun Xu (Pennsylvania State University) 2018

Dissertation committee for Weihang Wang (Purdue University) 2017

Dissertation committee for Steve T.K. Jan (Virginia Tech) 2017

Dissertation committee for Lannan Luo (Pennsylvania State University) 2017

Dissertation committee for Lei Tian (University of Colorado - Boulder) 2016

PC member for AAAI Conference on Artificial Intelligence (AAAI) 2020

PC member for ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2018

PC member for Annual Computer Security Applications Conference (ACSAC) 2019

PC member for IEEE Symposium on Security and Privacy (S&P) 2022, 2023

PC member for ACM Conference on Computer and Communications Security (CCS) 2017, 2018, 2019, 2020, 2021, 2022, 2023

PC member for USENIX Security Symposium (USENIX Security) 2019, 2020, 2021

PC member for World Wide Web Conference (WWW) 2017

PC member for Financial Cryptography and Data Security (FC) 2016

Review for Network and Distributed System Security Symposium (NDSS) 2014, 2015

Review for ACM Conference on Computer and Communications Security (CCS) 2012, 2013

Review for USENIX Symposium on Networked Systems Design and Implementation (NSDI) 2013

Review for World Wide Web Conference (WWW) 2014

Review for IEEE/IFIP Conference on Dependable Systems and Networks (DSN) 2010, 2014

Review for Annual Computer Security Applications Conference (ACSAC) 2013

Review for USENIX Symposium On Usable Privacy and Security (SOUPS) 2014

Review for ACM Conference on Mobile Systems, Applications, and Services (MOBISYS) 2010

Review for IEEE Conference on Computer Communications (INFOCOM) 2009, 2010

Review for IEEE Conference on Distributed Computing Systems (ICDCS) 2008, 2010