Heng Yin

Contact Information

Department of Computer Science and Engineering
UC Riverside
316 Winston Chung Hall
Riverside, CA 92521 USA

Voice: (951)827-6437

Fax: (951)827-4643
E-mail: heng@cs.ucr.edu
WWW: https://www.cs.ucr.edu/~heng

Research Interests

My research interests lie in computer security. In particular, I am interested in developing all kinds of techniques (such as program analysis, virtualization, and machine learning/deep learning) to solve computer and software security problems, including but not limited to malware detection and analysis, vulnerability discovery, program hardening, and digital forensics.

Education

The College of William and Mary, Williamsburg, VA, USA

Ph.D. student in Computer Science, (Graduation date: August 2009)

- Thesis Topic: Malware Detection and Analysis via Layered Annotative Execution
- Advisors: Haining Wang and Dawn Song (from UC Berkeley)

Huazhong University of Science and Technology, Wuhan, China

M.S., in Computer Engineering, June 2002

- Advisor: Zhitang Li
- Research Interests: Network Security

B.S in Computer Science and Engineering, June 1999

Professional Experience

UC Riverside, Riverside, CA

- *Tenured Associate Professor* **June 2016 to Present**

Syracuse University, Syracuse, NY

- *Tenured Associate Professor* **June 2015 to June 2016**
- *Tenure-track Assistant Professor* **September 2009 to May 2015**

University of California, Berkeley, Berkeley, CA

- *Research Assistant* **June 2008 to August 2009**

Carnegie Mellon University, Pittsburgh, PA

- *Research Assistant* **October 2005 to June 2008**

College of William and Mary, Williamsburg, VA

- *Research Assistant* **June 2004 to September 2005**

Books and Book Chapters

- Heng Yin and Dawn Song. Automatic Malware Analysis: An Emulator based Approach. Springer Briefs in Computer Science, September 2012.
- David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Pongsin Poosankam, Dawn Song, and Heng Yin. Automatically Identifying Trigger-based Behavior in Malware. Book Chapter in "Botnet Analysis in Defense", 2007.

Journals

- Andrew Henderson, Lok Kwong Yan, Xunchao Hu, Aravind Prakash, Heng Yin, and Stephen McCamant. DECAF: A Platform-Neutral Whole-System Dynamic Binary Analysis Platform, IEEE Transactions on Software Engineering, Vol 43, No. 2, February 2017.
- Aravind Prakash, Eknath Venkataramani, Heng Yin, and Zhiqiang Lin. On the Trustworthiness of Memory Analysis—An Empirical Study from the Perspective of Binary Execution. IEEE Transactions on Dependable and Secure Computing (TDSC), September 2015.
- Yufei Gu, Yangchun Fu, Aravind Prakash, Zhiqiang Lin, and Heng Yin. Multi-aspect, robust, and memory-exclusive guest os fingerprinting. IEEE Transactions on Cloud Computing, 2014.
- Heng Yin, Bo Sheng, Haining Wang, and Jianping Pan. Keychain-based signatures for securing bgp. IEEE Journal on Selected Areas in Communications (J-SAC), Internet Routing Scalability, October 2010.
- Mengjun Xie, Heng Yin, and Haining Wang. Thwarting Email Spam Laundering. ACM Transactions on Information and System Security, 2008 .
- Heng Yin and Haining Wang. Building an Application-aware IPsec Policy System. In the IEEE/ACM Transactions on Networking, December 2007.

Conferences and Workshops

- Xunchao Hu, Brian Testa, and Heng Yin, ChaffyScript: Vulnerability-Agnostic Defense of JavaScript Exploits via Memory Perturbation, in the 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm'19), October 2019.
- Jinghan Wang, Yue Duan, Wei Song, Heng Yin, and Chengyu Song, Be Sensitive and Collaborative: Analyzing Impact of Coverage Metrics in Greybox Fuzzing, in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID'19), September 2019.
- Ali Davanian, Zhenxiao Qi, Yu Qu, and Heng Yin, DECAF++: Elastic Whole-System Dynamic Taint Analysis, in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID'19), September 2019.
- Yue Duan, Lian Gao, Jie Hu, and Heng Yin, Automatic Generation of Non-intrusive Updates for Third-Party Libraries in Android Applications, in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID'19), September 2019.
- Yaowen Zheng, Ali Davanian, Heng Yin, Chengyu Song, Hongsong Zhu, and Limin Sun, Firm-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation, in the 28th USENIX Security Symposium, August 2019.

- Lei Zhao, Yue Duan, Heng Yin, and Jifeng Xuan. Send Hardest Problems My Way: Probabilistic Path Prioritization for Hybrid Fuzzing, in the Network and Distributed System Security Symposium (NDSS'19), February 2019. (Acceptance rate: 17.4%)

- Wei Song, Heng Yin, Chang Liu, and Dawn Song. DeepMem: Learning Graph Neural Network Models for Fast and Robust Memory Forensic Analysis, in the 25th ACM Conference on Computer and Communications Security (CCS'18), October 2018. (Acceptance rate: 16.6%)

- Ahmad Darki, Chun-Yu Chuang, Michalis Faloutsos, Zhiyun Qian, and Heng Yin. RARE: A Systematic Augmented Router Emulation for Malware Analysis, in Passive and Active Measurement Conference 2018 (PAM'18), March, 2018.

- Yue Duan, Mu Zhang, Abhishek Vasist Bhaskar, Heng Yin, Xiaorui Pan, Tongxin Li, Xueqiang Wang, and Xiaofeng Wang. Things You May Not Know About Android (Un)Packers: A Systematic Study based on Whole-System Emulation, in the Network and Distributed System Security Symposium (NDSS'18), February 2018. (Acceptance rate: 16.1%)

- Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, and Heng Yin. Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis, in the Network and Distributed System Security Symposium (NDSS'18), February 2018. (Acceptance rate: 16.1%)

- Xiaojun Xu, Chang Liu, Qian Feng, Heng Yin, Le Song and Dawn Song. Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection, in the 24th ACM Conference on Computer and Communications Security, October 2017 (CCS'17). (Acceptance rate: 18.06%)

- David Korczynski and Heng Yin. Capturing Malware Propagations with Code Injections and Code-Reuse Attacks, in the 24th ACM Conference on Computer and Communications Security (CCS'17), October 2017. (Acceptance rate: 18.06%)

- Xunchao Hu, Yao Cheng, Yue Duan, Andrew Henderson and Heng Yin. JSForce: A Forced Execution Engine for Malicious JavaScript Detection, in the 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm'17), October 2017.

- Andrew Henderson, Heng Yin, Guang Jin, Hao Han, and Hongmei Deng. VDF: Targeted Evolutionary Fuzz Testing of Virtual Devices, in the 20th International Symposium on Research on Attacks, Intrusions and Defenses (RAID'17), September 2017.

- Xudong He, Zhijiang Dong, Heng Yin and Yujian Fu. A Framework for Developing Cyber Physical Systems, appeared in the 29th International Conference on Software Engineering & Knowledge Engineering, July 2017. Best Paper Award

- Qian Feng, Minghua Wang, Mu Zhang, Rundong Zhou, Andrew Henderson, and Heng Yin. Extracting Conditional Formulas for Cross-Platform Bug Search, appeared in ACM Asia Conference on Computer and Communications Security (AsiaCCS'17), April 2017.

- Xiaorui Pan, Xueqiang Wang, Yue Duan, Xiaofeng Wang, and Heng Yin. Dark Hazard: Large-Scale Discovery of Unknown Hidden Sensitive Operations in Android Apps, appeared in the Network and Distributed System Security Symposium (NDSS'17), February 2017. (Acceptance rate: 16.1%)

- Qian Feng, Rundong Zhou, Chengcheng Xu, Yao Cheng, Brian Testa, and Heng Yin. Scalable Graph-based Bug Search for Firmware Images, in the 23rd ACM Conference on Computer and Communications Security (CCS'16), October 2016.
- Xunchao Hu, Aravind Prakash, Jinghan Wang, Rundong Zhou, Yao Cheng, and Heng Yin. Semantics-Preserving Dissection of JavaScript Exploits via Dynamic JS-Binary Analysis, in the 19th Symposium on Research in Attacks, Intrusions and Defenses (RAID'16), September 2016.
- Qian Feng, Aravind Prakash, Minghua Wang, Curtis Carmony and Heng Yin. ORIGEN: Automatic Extraction of Offset-Revealing Instructions for Cross-Version Memory Analysis, In Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (AsiaCCS'16), May 2016.
- Curtis Carmony, Mu Zhang, Xunchao Hu, Abhishek Vasisht Bhaskar, and Heng Yin, "Extract Me If You Can: Abusing PDF Parsers in Malware Detectors", in Proceedings of Network and Distributed System Security Symposium (NDSS'16), 2016.
- Aravind Prakash and Heng Yin, "Defeating ROP Through Denial of Stack Pivot", in Proceedings of 2015 Annual Computer Security Applications Conference (ACSAC'15), December 2015.
- Minghua Wang, Heng Yin, Abhishek Vasisht Bhaskar, Purui Su, and Dengguo Feng, "Binary Code Continent: Finer-Grained Control Flow Integrity for Stripped Binaries", in Proceedings of 2015 Annual Computer Security Applications Conference (ACSAC'15), December 2015.
- Mu Zhang, Yue Duan, Qian Feng, and Heng Yin, "Towards Automatic Generation of Security-Centric Descriptions for Android Apps", In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS'15), November 2015.
- Yue Duan, Mu Zhang, Heng Yin, and Yuzhe Tang, "Privacy-Preserving Offloading of Mobile App to the Public Cloud", In The 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud'15), Santa Clara, CA, July 2015.
- Aravind Prakash, Xunchao Hu, and Heng Yin. "vfGuard: Strict Protection for Virtual Function Calls in COTS C++ Binaries", In Proceedings of ISOC Network and Distributed System Security Symposium (NDSS'15), February 2015.
- Qian Feng, Aravind Prakash, Heng Yin, and Zhiqiang Lin. MACE: High-Coverage and Robust Memory Analysis For Commodity Operating Systems, In Annual Computer Security Applications Conference, New Orleans, Louisiana, December 8-12 2014.
- Mu Zhang, Yue Duan, Heng Yin, and Zhiruo Zhao. Semantics-aware android malware classification using weighted contextual api dependency graphs. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS'14), November 2014.
- Xing Jin, Xunchao Hu, Kailiang Ying, Wenliang Du, Heng Yin, and Gautam Nagesh Peri. Code injection attacks in html5-based mobile apps: Characterization, detection and mitigation. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS'14), November 2014.
- Xiaolei Li, Guangdong Bai, Benjamin Thian, Zhenkai Liang, and Heng Yin. A lightweight software environment for confining android malware. In Proceedings of the Eighth International Conference on Software Security and Reliability (SERE'14), Trustworthy Computing Workshop, July 2014.

- Andrew Henderson, Aravind Prakash, Lok Kwong Yan, Xunchao Hu, Xujiewen Wang, Rundong Zhou, and Heng Yin. Make it work, make it right, make it fast: building a platform-neutral whole-system dynamic binary analysis platform. In Proceedings of the International Symposium on Software Testing and Analysis (ISSTA'14), San Jose, CA, July 2014.

- Mu Zhang and Heng Yin. Efficient, Context-Aware Privacy Leakage Confinment for Android Applications without Firmware Modding. In Proceedings of the 9th ACM Symposium on Information, Computer and Communication Security, Kyoto, Japan, June 2014.

- Mu Zhang and Heng Yin. AppSealer: Automatic generation of vulnerability-specific patches for preventing component hijacking attacks in Android applications. In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14), February 2014.

- Yousra Aafer, Wenliang Du, and Heng Yin. DroidAPIMiner: Mining API-level features for robust malware detection in Android. In Proceedings of the 9th International Conference on Security and Privacy in Communication Networks (SecureComm'13), September 2013.

- Aravind Prakash, Eknath Venkataramani, Heng Yin, and Zhiqiang Lin. Manipulating semantic values in kernel data structures: Attack assessments and implications. In Proceedings of the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'13), June 2013.

- Aravind Prakash, Heng Yin, and Zhenkai Liang. Enforcing system-wide control flow integrity for exploit detection and diagnosis. In Proceedings of the 8th ACM Symposium on Information, Computer and Communication Security, May 2013.

- Yufei Gu, Yangchun Fu, Aravind Prakash, Zhiqiang Lin, and Heng Yin. OS-Sommelier: Memory-only operating system fingerprinting in the cloud. In Proceedings of the 3rd ACM Symposium on Cloud Computing (SOCC'12), October 2012.

- Lok-Kwong Yan and Heng Yin. DroidScope: Seamlessly reconstructing os and dalvik semantic views for dynamic android malware analysis. In Proceedings of the 21st USENIX Security Symposium, August 2012.

- Lok-Kwong Yan, Manjukumar Jayachandra, Mu Zhang, and Heng Yin. V2E: Combining hardware virtualization and software emulation for transparent and extensible malware analysis. In Proceedings of the Eighth Annual International Conference on Virtual Execution Environments (VEE'12), March 2012.

- Lok-Kwong Yan, Manjukumar Jayachandra, Mu Zhang, and Heng Yin. Transparent and extensible malware analysis by combining hardware virtualization and software emulation. In Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS'12), Invited Paper, February 2012.

- Mingwei Zhang, Aravind Prakash, Xiaolei Li, Zhenkai Liang, and Heng Yin. Identifying and analysing pointer misuses for sophisticated memory-corruption exploit diagnosis. In Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS'12), February 2012.

- Tongbo Luo, Hao Hao, Wenliang Du, Yifei Wang, and Heng Yin. Attacks on webview in the android system. In Proceedings of the 27th Annual Computer Security Application Conference (ACSAC'11), December 2011.

- Heng Yin, Pongsin Poosankam, Steve Hanna, and Dawn Song. HookScout: Proactive binary-centric hook detection. In Proceedings of Seventh Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA'10), July 2010.

- Min Gyung Kang, Heng Yin, Steve Hanna, Stephen McCamant, and Dawn Song. Emulating Emulation-Resistant Malware. In the 2nd Workshop on Virtual Machine Security (VMSec), November 2009.

- Heng Yin, Zhenkai Liang, and Dawn Song. HookFinder: Identifying and Understanding Malware Hooking Behaviors. In the Proceedings of the 15th Annual Network and Distributed System Security Symposium, February 2008.

- Min Gyung Kang, Pongsin Poosankam, and Heng Yin. Renovo: A Hidden Code Extractor for Packed Executables. In the Proceedings of the 5th ACM Workshop on Recurring Malcode, November 2007.

- Juan Caballero, Heng Yin, Zhenkai Liang, and Dawn Song. Polyglot: Automatic Extraction of Protocol Message Format using Dynamic Binary Analysis. In the Proceedings of the 14th ACM Conference on Computer and Communication Security, October 2007.

- Heng Yin, Dawn Song, Manual Egele, Christopher Kruegel, and Engin Kirda. Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis. In the Proceedings of the 14th ACM Conference on Computer and Communication Security, October 2007.

- Heng Yin, Bo Sheng, Haining Wang, and Jianping Pan. Securing BGP through Keychain-based Signatures. In Proceedings of the 15th IEEE International Workshop on Quality of Service, June 2007.

- Manual Egele, Christopher Kruegel, Engin Kirda, Heng Yin, and Dawn Song. Dynamic Spyware Analysis. In the Proceedings of the 2007 USENIX Annual Technical Conference, June 2007

- Mengjun Xie, Heng Yin, and Haining Wang. An Effective Defense Against Email Spam Laundering. In the Proceedings of the 13th ACM Conference on Computer and Communication Security, October 2006.

- Heng Yin and Haining Wang. Building an Application-aware IPsec Policy System. In the Proceedings of the 14th USENIX Security Symposium, August 2005.

Technical Reports

- Heng Yin and Dawn Song. Temu: Binary code analysis via whole-system layered annotative execution. Technical Report UCB/EECS-2010-3, EECS Department, University of California, Berkeley, January 2010.

- Heng Yin, Zhenkai Liang, and Dawn Song. HookFinder: Identifying and Understanding Malware Hooking Behaviors. cmu-cylab-07-015, CyLab, Carnegie Mellon University, October 17, 2007.

- David Brumley, Cody Hartwig, Min Gyuang Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam, Dawn Song, and Heng Yin. BitScope: Automatically Dissecting Malicious Binaries. Technical Report CMU-CS-07-133, School of Computer Science, Carnegie Mellon University, March 2007.

Teaching Experience

Courses offered at UC Riverside

- CS 153 Design of Operating System: F18
- CS 202 Advanced Operating System: S19, S18, F17, S17
- CS 260 Seminar in Computer Science: W19, W17

Courses offered at Syracuse University

- CIS 341 Computer Organization and Programming Systems: Spring 2016, Spring 2015, Spring 2014, Spring 2013, Fall 2011, Fall 2010
- CIS 700/CSE 791 Program Analysis for Software Security: Fall 2015
- CIS 700/CSE 791 Mobile Operating Systems: Fall 2014, Fall 2013, Fall 2012
- CIS 700/CSE 791 Software Security and Malware Defense: Spring 2014, Spring 2013, Spring 2011, Spring 2010
- CIS 700/ CSE 791 Advanced Topics in Mobile Systems: Spring 2011
- Trusted Computing at AFRL: Summer 2010

Awards & Grants

- (PI) Adversarial Learning on Malware Classifiers, gift fund from Avast, Inc. (07/15/2019 onward), $74,555
- (PI) Building an efficient DECAF-based Fault Injection Framework, subcontract from Los Alamos National Lab, sponsored by DoE, (10/5/2017 to 7/31/2018), $80,000
- (PI) Leapfrog: Learn and Prune Features in Binary Programs, sponsored by ONR, (9/30/2017 to 9/30/2022), $4,686,131 (Due to COI, now serve as senior personnel)
- (PI) SaTC: CORE: Small: Towards Robust and Scalable Search of Binary Code and Data, sponsored by NSF, (9/15/2017 to 8/31/2020), $476,756
- (PI) Interfaces, Models, and Monitoring for Resource-aware Transformations that Augment the Lifecycle of Systems (IMMoRTALS), sponsored by DARPA, subcontract from Raytheon BBN (10/2015 to 11/2019), $536,803
- (PI) A Virtualization Framework for Fault Injection, subcontract from Los Alamos National Lab, sponsored by DoE, (04/2015 to 03/2016), $81,088
- (PI) A Runtime Checker with Evolutionary Algorithm Decision Making, sponsored by Air Force Research Lab, subcontract from Alabama A&M, (04/2015 - 03/2018), $315,000
- (PI) CodeJitsu: Automated Binary Analysis and Hardening for Cyber Defense, sponsored by DARPA, subcontracted from UC Berkeley, (06/2014 to 08/2016), $160,000
- (PI) Mcafee: Automatic Malware Analysis (08/2012 to 07/2015), $163,106.
- (PI) NSF Career Award: Binary and Virtualization Centric Malware Defense (08/2011 to 07/2016), $550,000

- (PI) NSF Trustworthy Computing Program: Mining Operating System Semantics (08/2010 to 08/2013), $429,000
- SIGCOMM 2005 Student Travel Grant
- USENIX Security Symposium 2005 Student Stipend Award

Professional Activities & Services

Organizers

- Poster/Demo Chair, ACM Conference on Computer and Communications Security (CCS), 2017
- Workshop Chair, ACM Symposium on Information, Computer and Communication Security (ASIACCS), 2016
- Technical Committee, International Forum for Security Research
- Associate Editor, Cybersecurity

Program Committees

- ACM Conference on Computer and Communications Security (CCS): 2012 (Poster Session), 2014, 2017, 2018, 2019
- Annual Computer Application Security Conference (ACSAC): 2014, 2015, 2017, 2018, 2019
- ACM Symposium on Information, Computer and Communication Security (ASIACCS), 2017, 2018, 2019, 2020
- ACM WiSec 2016
- ISOC Network and Distributed System Security Symposium (NDSS): 2013, 2015 Security and Privacy in Communication Networks
- (SecureComm): 2011, 2013, 2014, 2015
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2012, 2019
- IEEE Cybersecurity Development Conference (SecDev): 2018
- IPCCC: 2013

Panelists

- NSF SaTC 2015, 2016, 2018
- NSF SHF 2017
- DHS 2016

Reviewer for journals

- Transactions on Computers
- Transactions on Information Forensics and Security
- Transactions on Dependable and Secure Computing
- International Journal of Communication Systems
- Ad Hoc & Sensor Wireless Network Journal
- International Journal of Information Security
- Security and Communication Networks
- ACM Transactions on Programming Languages and Systems
- ACM Computing Surveys

External reviewer for conferences

- IEEE Security & Privacy (Oakland) 2008
- ACM Conference on Computer and Communication Security (CCS) 2006
- USENIX Security Symposium 2006
- Network and Distributed System Security Symposium (NDSS) 2006 2009

- USENIX Symposium on Operating Systems Design and Implementation (OSDI) 2006
- EuroSys 2007
- IEEE InfoCom 2007 2008 2009
- International Conference on Distributed Computing Systems (ICDCS) 2006 2008