

Chengyu Song

314 Winston Chung Hall
csong@cs.ucr.edu · +1 (951) 827-5478 · <https://www.cs.ucr.edu/~csong/>
[Google Scholar Profile](#) · [GitHub](#)

| | | |
|----------------------------|--|----------------|
| ACADEMIC POSITION | Assistant Professor , CSE, UC Riverside | 2016 – Present |
| RESEARCH INTERESTS | System Security, Program Analysis and Verification, Operating Systems, Architecture | |
| EDUCATION | Georgia Institute of Technology , Atlanta, Georgia, USA | |
| | Ph.D., Computer Science · Advisors: Wenke Lee and Taesoo Kim | 2010 – 2016 |
| | Peking University , Beijing, China | |
| | M.Eng., Computer Applied Technology · Advisors: Jianwei Zhuge and Zhiyuan Ye | 2007 – 2010 |
| | B.S., Computer Science and Technology · Graduated with Honor. | 2003 – 2007 |
| HONORS & AWARDS | RAID'19 Best Paper | 2019 |
| | WOOT'18 Best Paper | 2018 |
| | Finalist to DARPA Cyber Grand Challenge (Disekt) | 2016 |
| | CSAW Best Applied Research Paper, 3rd Place & Finalist (2 papers) | 2015 |
| | 2015 Internet Defense Prize (\$100k), | 2015 |
| RESEARCH EXPERIENCE | UC Riverside , Department of Computer Science and Technology Tenure-track Assistant Professor | 2016 – Present |
| | Georgia Institute of Technology , College of Computing Graduate Research Assistant · Projects: Defense Techniques against Memory Corruption Attacks, Automated Program Patching and Hardening, Vulnerability Discovery, Privacy Protection · Advisor: Wenke Lee and Taesoo Kim | 2010 – 2016 |
| | Samsung Research American , Knox Team Research Intern · Project: Kernel Control Flow Hijacking Detection through ARM CoreSight ETM · Supervisor: Ahmed Moneeb Azab | 2014 |
| | Samsung Telecommunications American , Knox Team Research Intern · Project: Hypervisor for ARM based Smartphones · Supervisor: Ahmed Moneeb Azab | 2013 |
| | Microsoft Research , Redmond, Security and Privacy Research Intern · Project: CloudShot, Fast Snapshotting Service for the Cloud Infrastructure · Supervisor: Weidong Cui and Marcus Peinado | 2012 |
| | Microsoft Research , eXtreme Computing Group Research Intern · Project: Trusted Passage, Enabling Trustworthy End-to-End Communication in the Cloud · Supervisor: Himanshu Raj | 2011 |

- Projects: Botnet Monitoring, Distributed HoneyNet, Malware Analysis, Honeyfarm, Drive-by Download Attack Detection and Prevention
- Advisor: Jianwei Zhuge and Zhiyuan Ye

PUBLICATIONS

JOURNALS

Stopping Memory Disclosures via Diversification and Replicated Execution.

Kangjie Lu, Meng Xu, Chengyu Song, Taesoo Kim, and Wenke Lee.
IEEE Transactions on Dependable and Secure Computing (TDSC), Oct 2018.

Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques.

Meng Xu, Chengyu Song, Yang Ji, Ming-Wei Shih, Kangjie Lu, Cong Zheng, Ruian Duan, Yeongjin Jang, Byoungyoung Lee, Chenxiong Qian, Sangho Lee, and Taesoo Kim.
ACM Computing Surveys (CSUR), vol. 49, no. 2, pp. 38:1–38:47, Aug 2016.

CONFERENCES AND WORKSHOPS

UBITect: A Precise and Scalable Method to Detect Use-Before-Initialization bugs in Linux Kernel.

Yizhuo Zhai, Yu Hao, Hang Zhang, Daimeng Wang, Chengyu Song, Zhiyun Qian, Mohsen Lesani, Srikanth V. Krishnamurthy, and Paul Yu. In *Proceedings of the 2020 ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*, 2020. Acceptance rate: 28.05% (101 of 360).

CrFuzz: Fuzzing Multi-purpose Programs through Input Validation.

Suhwan Song, Chengyu Song, Yeongjin Jang, and Byoungyoung Lee.
In *Proceedings of the 2020 ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*, 2020. Acceptance rate: 28.05% (101 of 360).

SpecROP: Speculative Exploitation of ROP Chains.

Atri Bhattacharyya, Andres S. Marin, Esmaeil M. Koruyeh, Nael Abu-Ghazaleh, Chengyu Song, and Mathias Payer. In *Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2020. Acceptance rate: 25.62% (31 of 121).

Connecting the Dots: Detecting Adversarial Perturbations Using Context Inconsistency.

Shasha Li, Shitong Zhu, Sudipta Paul, Amit K. Roy-Chowdhury, Chengyu Song, Srikanth V. Krishnamurthy, Ananthram Swami, and Kevin S. Chan. In *Proceedings of the 16th European Conference on Computer Vision (ECCV)*, 2020. Acceptance rate: 27.08% (1361 of 5025), poster presentation.

SPECCFI: CFI Informed Branch Prediction.

Esmaeil M. Koruyeh, Shirin H. Shirazi, Khaled N. Khaswaneh, Chengyu Song, and Nael Abu-Ghazaleh. In *Proceedings of the 41st IEEE Symposium on Security and Privacy (Oakland)*, 2020. Acceptance rate: 12.37% (104 of 841).

KLOTSKI: Efficient Obfuscated Execution against Controlled-Channel Attacks.

Pan Zhang, Chengyu Song, Heng Yin, Deqing Zou, Elaine Shi, and Hai Jin.
In *Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2020. Acceptance rate: 18%.

SymTCP: Eluding Stateful Deep Packet Inspection with Automated Discrepancy Discovery.

Zhongjie Wang, Shitong Zhu, Yue Cao, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Tracy D. Braun, and Kevin S. Chan. In *Proceedings of the 2020 Network and Distributed System Security Symposium (NDSS)*, 2020. Acceptance rate: 17.4%.

RENN: Efficient Reverse Execution with Neural-Network-assisted Alias Analysis.

Dongliang Mu, Wenbo Guo, Alejandro Cuevas, Yueqi Chen, Jinxuan Gai, Xinyu Xing, Bing Mao, and Chengyu Song. In *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2019. Acceptance rate: 20.45% (91 of 445).

Principled Unearthing of TCP Side Channel Vulnerabilities.

Yue Cao, Zhongjie Wang, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, and Paul Yu. In *Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS)*, 2019. Acceptance rate: 15.97% (149 of 933).

Be Sensitive and Collaborative: Analyzing Impact of Coverage Metrics in Greybox Fuzzing.

Jinghan Wang, Yue Duan, Wei Song, Heng Yin, and Chengyu Song. In *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019. Acceptance rate: 22.29% (36 of 166).

Firm-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation.

Yaowen Zheng, Ali Davanian, Heng Yin, Chengyu Song, Hongsong Zhu, and Limin Sun. In *Proceedings of the 28th USENIX Security Symposium (Security)*, 2019. Acceptance rate: 15.27% (113 of 740).

SafeSpec: Banishing the Spectre of a Meltdown with Leakage-Free Speculation.

Khaled N. Khasawneh, Esmaeil M. Koruyeh, Chengyu Song, Dmitry Evtvushkin, Dmitry Ponomarev, and Nael Abu-Ghazaleh. In *Proceedings of the 56th Design Automation Conference (DAC)*, 2019. Acceptance rate: 21.15% (158 of 747).

Figment: Fine-grained Permission Management for Mobile Apps.

Ioannis Gasparis, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Rajiv Gupta, and Paul Yu. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2019. Acceptance rate: 19.67% (288 of 1464).

Stealthy Adversarial Perturbations Against Real-Time Video Classification Systems.

Shasha Li, Ajaya Neupane, Sujoy Paul, Chengyu Song, Srikanth V. Krishnamurthy, Amit K. Roy Chowdhury, and Ananthram Swami. In *Proceedings of the 2019 Network and Distributed System Security Symposium (NDSS)*, 2019. Acceptance rate: 17.08% (89 of 521).

IoTSan: Fortifying the Safety of IoT Systems.

Dang Tu Nguyen, Chengyu Song, Zhiyun Qian, Srikanth V. Krishnamurthy, Edward J. M. Colbert, and Patrick McDaniel. In *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNext)*, 2018. Acceptance rate: 17.30% (32 of 185).

IAC: On the Feasibility of Utilizing Neural Signals for Access Control.

Md Lutfor Rahman, Ajaya Neupane, and Chengyu Song. In *Proceedings of the 2018 Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance rate: 20.10% (60 of 299).

Learning Tensor-based Representations from Brain-Computer Interface Data for Cybersecurity.

Md. Lutfor Rahman*, Sharmistha Bardhan*, Ajaya Neupane, Evangelos E. Papalexakis, and Chengyu Song. In *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD)*, 2018. Acceptance rate: 27.28% (39 of 143).

Spectre Returns! Speculation Attacks using the Return Stack Buffer.

Esmaiel M. Koruyeh, Khaled N. Khasawneh, Chengyu Song, and Nael Abu-Ghazaleh. In *Proceedings of the 12th USENIX Workshop on Offensive Technologies (WOOT)*, 2018.

Best Paper.

Droid M+: Developer Support for Imbibing Android's New Permission Model.

Ioannis Gasparis, Azeem Aqil, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Rajiv Gupta, and Edward Colbert. In *Proceedings of the 13th ACM ASIA Conference on Information, Computer and Communications Security (AsiaCCS)*, 2018. Acceptance rate: 20.0% (62 of 310).

Enhancing Memory Error Detection for Large-Scale Applications and Fuzz Testing.

Wookhyun Han, Byunggill Joe, Byoungyoung Lee, Chengyu Song, and Insik Shin. In *Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS)*, 2018. Acceptance rate: 21.5% (71 of 331).

Your State is Not Mine: A Closer Look at Evading Stateful Internet Censorship.
Zhongjie Wang, Yue Cao, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy.
In *Proceedings of the 2017 ACM Internet Measurement Conference (IMC)*, 2017.
Acceptance rate: 28.0% (28 of 100).

Detecting Android Root Exploits by Learning from Root Providers.
Ioannis Gasparis, Zhiyun Qian, Chengyu Song, and Srikanth V. Krishnamurthy.
In *Proceedings of the 26th USENIX Security Symposium (Security)*, 2017.
Acceptance rate: 16.3% (85 of 522).

Efficient Protection of Path-Sensitive Control Security.
Ren Ding, Chenxiong Qian, Chengyu Song, William R. Harris, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 26th USENIX Security Symposium (Security)*, 2017.
Acceptance rate: 16.3% (85 of 522).

UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leakages.
Kangjie Lu, Chengyu Song, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
Acceptance rate: 16.5% (137 of 831).

HDFI: Hardware-assisted Data-Flow Isolation.
Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (Oakland)*, 2016. Acceptance rate: 13.8% (55 of 400).

Enforcing Kernel Security Invariants with Data Flow Integrity.
Chengyu Song, Byoungyoung Lee, Kangjie Lu, William R. Harris, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS)*, 2016.
Acceptance rate: 15.4% (60 of 389).

VTrust: Regaining Trust on Virtual Calls.
Chao Zhang, Scott A. Carr, Tongxin Li, Yu Ding, Chengyu Song, Mathias Payer, and Dawn Song.
In *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS)*, 2016.
Acceptance rate: 15.4% (60 of 389).

ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks.
Kangjie Lu, Chengyu Song, Byoungyoung Lee, Simon P. Chung, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.
Acceptance rate: 19.9% (128 of 646).

Cross-checking Semantic Correctness: The Case of Finding File System Bugs.
Changwoo Min, Sanidhya Kashyap, Byoungyoung Lee, Chengyu Song, and Taesoo Kim.
In *Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP)*, 2015.
Acceptance rate: 16.1% (30 of 186).

Type Casting Verification: Stopping an Emerging Attack Vector.
Byoungyoung Lee, Chengyu Song, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 24th USENIX Security Symposium (Security)*, 2015.
Acceptance rate: 15.7% (67 of 426). **2015 Internet Defense Prize**

JITScope: Protecting Web Users from Control-Flow Hijacking Attacks.
Chao Zhang, Mehrdad Niknami, Kevin Zhijie Chen, Chengyu Song, Zhaofeng Chen, and Dawn Song.
In *Proceedings of the 34th Annual IEEE International Conference on Computer Communications (INFOCOM)*, 2015. Acceptance rate: 19.2% (316 of 1640).

Exploiting and Protecting Dynamic Code Generation.
Chengyu Song, Chao Zhang, Tielei Wang, Wenke Lee, and David Melski.
In *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*, 2015.
Acceptance rate: 16.9% (51 of 302).

VTint: Protecting Virtual Function Tables' Integrity.

Chao Zhang, Chengyu Song, Kevin Zhijie Chen, Zhaofeng Chen, and Dawn Song.
In *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*, 2015.
Acceptance rate: 16.9% (51 of 302).

Preventing Use-after-free with Dangling Pointers Nullification.

Byoungyoung Lee, Chengyu Song, Yeongjin Jang, Tielei Wang, Taesoo Kim, Long Lu, and Wenke Lee.
In *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*, 2015.
Acceptance rate: 16.9% (51 of 302). **CSAW 2015 Best Applied Research Paper (3rd place)**

A11y Attacks: Exploiting Accessibility in Operating Systems.

Yeongjin Jang, Chengyu Song, Simon P. Chung, Tielei Wang, and Wenke Lee.
In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, 2014.
Acceptance rate: 19.5% (114 of 585).

Mimesis Aegis: A Mimicry Privacy Shield.

Billy Lau, Pak Ho Chung, Chengyu Song, Yeongjin Jang, Wenke Lee, and Alexandra Boldyreva.
In *Proceedings of the 23rd USENIX Security Symposium (Security)*, 2014.
Acceptance rate: 19.1% (67 of 350).

Abusing Performance Optimization Weaknesses to Bypass ASLR.

Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 2014 BlackHat USA*, 2014.

Diagnosis and Emergency Patch Generation for Integer Overflow Exploits.

Tielei Wang, Chengyu Song, and Wenke Lee.
In *Proceedings of the 11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2014. Acceptance rate: 23.3% (14 of 60).

Mactans: Injecting Malware Into iOS Devices via Malicious Chargers.

Billy Lau, Yeongjin Jang, Chengyu Song, Tielei Wang, Pak Ho Chung, and Paul Royal.
In *Proceedings of the 2013 BlackHat USA*, 2013.

Flowers for Automated Malware Analysis.

Chengyu Song and Paul Royal.
In *Proceedings of the 2012 BlackHat USA*, 2012.

Impeding Automated Malware Analysis with Environment-sensitive Malware.

Chengyu Song, Paul Royal, and Wenke Lee.
In *Proceedings of the 7th USENIX conference on Hot topics in Security (HotSec)*, 2012.

Preventing Drive-by Download via Inter-Module Communication Monitoring.

Chengyu Song, Jianwei Zhuge, Xinhui Han, and Zhiyuan Ye.
In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, 2010. Acceptance rate: 15.1% (25 of 166).

Studying Malicious Websites and the Undergrounding Economy on the Chinese Web.

Jianwei Zhuge, Thorsen Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, and Wei Zou.
In *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS)*, 2008.

Collecting Autonomous Spreading Malware Using High-interaction Honeypot.

Jianwei Zhuge, Thorsen Holz, Xinhui Han, Chengyu Song, and Wei Zou.
In *Proceedings of the 9th International Conference on Information and Communications Security (ICICS)*, 2007.

PATENTS

Systems and Methods of Safeguarding User Information while Interacting with Online Service Providers. Wenke Lee, Alexandra Boldyreva, Chung Pak Ho, Billy Lau, and Chengyu Song. 2017.

Fast and Secure Virtual Machine Memory Checkpointing.

Weidong Cui, Marcus Peinado, and Chengyu Song. 2013.

| | | |
|---|--|---|
| TEACHING EXPERIENCE | Computer Security (CS 255) , CSE, UC Riverside Instructor | 2018W, 2018F, 2020W |
| | Computer Security (CS 165) , CSE, UC Riverside Instructor | 2017F |
| | Design of Operating Systems (CS 153) , CSE, UC Riverside Instructor | 2017S, 2018S, 2019S, 2019F |
| | Compiler Design (CS 152) , CSE, UC Riverside Instructor | 2019W |
| | Information Security Lab , CSE, UC Riverside Instructor | 2017W |
| | Network Hacking and Defense: Technology and Practice , EECS, Peking University Teaching Assistant and Guest Lecturer <ul style="list-style-type: none"> · Graduate and senior-undergraduate level course. · Instructor: Jianwei Zhuge | 2008 |
| SERVICE | TECHNICAL PROGRAM COMMITTEE | |
| | ACM Asia Conference on Computer and Communications Security (ASIACCS) | 2018, 2019, 2020 |
| | ACM Computer and Communications Security (CCS) | 2017, 2018, 2019 |
| | JOURNAL REVIEWER | |
| | IEEE Transactions on Dependable and Secure Computing | 2013, 2016, 2017, 2018 |
| | IEEE Transactions on Software Engineering | 2019 |
| | IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems | 2019 |
| | IEEE Transactions on Computers | 2018 |
| | IEEE Communications Letters | 2013 |
| | ACM Transaction on Privacy and Security | 2019 |
| | EXTERNAL REVIEWER | |
| | Design Automation Conference | 2019 |
| | USENIX Annual Technical Conference | 2018 |
| | ACM Computer and Communications Security (CCS) | 2013, 2015, 2016 |
| | USENIX Security Symposium | 2011, 2016 |
| | ISOC Network and Distributed System Security Symposium (NDSS) | 2015, 2016 |
| | USENIX Symposium on Network Systems Design and Implementations (NSDI) | 2013 |
| | European Symposium on Research in Computer Security (ESORICS) | 2012, 2013, 2014, 2015 |
| | Annual Computer Security Applications Conference (ACSAC) | 2013 |
| | Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) | 2011 |
| | Conference on Dependable Systems and Networks (DSN) | 2012 |
| | International Symposium on Engineering Secure Software and Systems (ESSOS) | 2015 |
| | REFERENCES | Prof. Wenke Lee, Ph.D. (advisor) The John P. Imlay Jr. Professor, College of Computing, Georgia Institute of Technology Co-Director, Institute for Information Security & Privacy, Georgia Institute of Technology |
| Prof. Taesoo Kim, Ph.D. (co-advisor) Catherine M. and James E. Allchin Early Career Assistant Professor, College of Computing, Georgia Institute of Technology | | |
| William R. Harris, Ph.D. Galois, Inc. | | |

Weidong Cui, Ph.D.
Senior Researcher, Microsoft Research Redmond

[compiled on 2020-07-21]