Chengyu Song

266 Ferst Drive, KACB RM 3108, Atlanta, GA 30332, USA
csong84@gatech.edu • +1 (404) 368-0189 • http://www.cc.gatech.edu/grads/c/csong43/
Google Scholar Profile • GitHub

RESEARCH INTERESTS Security and Privacy, Program Analysis, Operating Systems

EDUCATION

Georgia Institute of Technology, Atlanta, Georgia, USA

Ph.D., Computer Science — 2010 – 2016 (Expected)
- Advisors: Wenke Lee and Taesoo Kim

Peking University, Beijing, China

M.Eng., Computer Applied Technology — 2007 – 2010
- Advisors: Jianwei Zhuge and Zhiyuan Ye

B.S., Computer Science and Technology — 2003 – 2007
- Graduated with Honor.

PUBLICATIONS

PEER REVIEWED CONFERENCES AND WORKSHOPS

20. **HDFI: Hardware-assisted Data-Flow Isolation** (to appear).
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).*

19. **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).

18. **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).

17. **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).

16. **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).

15. **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**

14. **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).*

13. **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).

12. **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).

11. **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)**

10. **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).

9. **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).

8. **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.

7. **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).*

6. **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.

5. **Flowers for Automated Malware Analysis**.
Chengyu Song and Paul Royal.
In *Proceedings of the 2012* **BlackHat USA**, 2012.

4. **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.

3. **Preventing Drive-by Download via Inter-Module Communication Monitoring**.
Chengyu Song, Jianwei Zhuge, Xinhui Han, and Zhiyuan Ye.
In *Proceedings of the 15th ACM Symposium on Information, Computer and Communications Security* (**AsiaCCS**), 2010. *Acceptance rate: 15.1% (25 of 166).*

2. **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.

1. **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. 2014.

Fast and Secure Virtual Machine Memory Checkpointing.
Weidong Cui, Marcus Peinado, and Chengyu Song. 2013.

RESEARCH EXPERIENCE

Georgia Institute of Technology, College of Computing — 2010 – Present
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

Samsung Research American, Knox Team — 2014
Research Intern
- Project: Kernel Control Flow Hijacking Detection through ARM CoreSight ETM
- Supervisor: Ahmed Moneeb Azab

Samsung Telecommunications American, Knox Team — 2013
Research Intern
- Project: Hypervisor for ARM based Smartphones
- Supervisor: Ahmed Moneeb Azab

Microsoft Research, Redmond, Security and Privacy — 2012
Research Intern
- Project: CloudShot, Fast Snapshotting Service for the Cloud Infrastructure
- Supervisor: Weidong Cui and Marcus Peinado

Microsoft Research, eXetreme Computing Group — 2011
Research Intern
- Project: Trusted Passage, Enabling Trustworthy End-to-End Communication in the Cloud
- Supervisor: Himanshu Raj

Peking University, Institute of Computer Science and Technology — 2005 – 2010
Research Assistant
- Projects: Botnet Monitoring, Distributed Honeynet, Malware Analysis, Honeyfarm, Drive-by Download Attack Detection and Prevention
- Advisor: Jianwei Zhuge and Zhiyuan Ye

TEACHING EXPERIENCE

Network Hacking and Defense: Technology and Practice, EECS, Peking University — 2008
Teaching Assistant and Guest Lecturer
- Graduate and senior-undergraduate level course.
- Instructor: Jianwei Zhuge

HONORS & AWARDS

Internet Defense Prize, 2015
CSAW Best Applied Research Paper, 3rd Place & Finalist 2015
Okamatsu Scholarship 2009
Wangxuan Scholarship (First Rank) 2007

SERVICE

JOURNAL REVIEWER

IEEE Transactions on Dependable and Secure Computing 2013
IEEE Communications Letters 2013

EXTERNAL REVIEWER

Computer and Communications Security (CCS) 2013, 2015
USENIX Security Symposium 2011, 2015
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)
Full Professor, College of Computing, Georgia Institute of Technology
Co-Director, Institute for Information Security & Privacy, Georgia Institute of Technology
wenke@cc.gatech.edu +1 (404) 385-2879

Prof. Taesoo Kim, Ph.D. (co-advisor)
Assistant Professor, College of Computing, Georgia Institute of Technology
taesoo@gatech.edu +1 (404) 385-2934

Prof. William R. Harris, Ph.D.
Assistant Professor, College of Computing, Georgia Institute of Technology
wharris@cc.gatech.edu +1 (608) 807-4563

Weidong Cui, Ph.D.
Senior Researcher, Microsoft Research Redmond
wdcui@microsoft.com +1 (425) 421-7749

Chao Zhang, Ph.D.
Post-doc Researcher, Department of Electrical Engineering and Computer Sciences, UC Berkeley
chaoz@berkeley.edu +1 (510) 931-8372

[*compiled on 2016-03-04*]