Tiffany Bao, Ph.D.

**Education**

Carnegie Mellon University Computer Engineering Ph.D. 2018

Peking University Computer Science B.S. 2012

**Professional Appointments**

2018-present Assistant Professor, School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ

**Selected Awards**

National Security Agency Annual Scientific Paper Award, 2018.

USENIX HotSec Awarded Talk, 2017.

Carnegie Mellon University Presidential Fellowship, 2017.

VARA Outstanding Paper Award, 2012.

**Current Research Sponsors**

Defense Advanced Research Projects Agency, 2018-2025.

National Security Agency, 2019-2022.

Army Research Office, 2019-2020.

**Publications**

1. P. Zhang, A. Oest, H. Cho, Z. Sun, R.C. Johnson, B. Wardman, S. Sarker, A. Kapravelos, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupé, and G. Ahn, “CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing”, to appear in *Proceedings of the 42th IEEE Symposium on Security and Privacy (S&P ’21).*
2. Y. Wang, X. Jia, Y. Liu, K. Zeng, T. Bao, D. Wu, P. Su, “Not All Coverage Measurements Are Equal: Fuzzing by Coverage Accounting for Input Prioritization”, in *the Network and Distributed System Security Symposium (NDSS ’20)*.
3. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues.  
   F. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G. Ahn, in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19).*
4. Z. Sun, C. Rubio-Medrano, Z. Zhao, T. Bao, A. Doupé and G. Ahn, “Understanding and Predicting Private Interactions in Underground Forums”, in *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY ’19)*.
5. T. Bao, R. Wang, Y. Shoshitaishvili, and D. Brumley, “Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits”, in *Proceedings of the 38th IEEE Symposium on Security and Privacy (S&P ’17)*.
6. T. Bao, Y. Shoshitaishvili, R. Wang, C. Kruegel, G. Vigna and D. Brumley, “How Shall We Play a Game: A Game-theoretical Model for Cyber-warfare”, in *Proceedings of the 30th IEEE Computer Security Foundations (CSF ’17)*. **National Security Agency Annual Scientific Paper Award.**
7. T. Bao, “Security is a Game”, in *2017 USENIX Summit on Hot Topics in Security (HotSec ’17)*. **USENIX HotSec Awarded Talk.**
8. T. Bao, Y. Shoshitaishvili, R. Wang and D. Brumley, “A Game-theoretical Model for Cyber-warfare Games (Invited Poster)”, *in the 8th Workshop on Computational Cybersecurity in Compromised Environments (C3E ’16).*
9. T. Bao, J. Burket, M. Woo, R. Turner, and D. Brumley, “ByteWeight: Learning to Recognize Functions in Binary Code”, in *Proceedings of the 23rd USENIX Security Symposium (USENIX ’14)*.
10. L. Chen, J. Zhuge, F. Tian, T. Bao, and X. Lu, “Type-based Dynamic Taint Analysis Technology”, in *Tsinghua Science and Technology Journal*, 2012.
11. L. Chen, J. Zhuge, F. Tian, T. Bao, and X. Lu, “Toward Type-based Dynamic Taint Analysis”, in *Proceedings of the 5th Conference of Vulnerability Analysis and Risk Assessment (VARA ’12)*. **Outstanding Paper Award.**
12. T. Bao, T. Avgerinos, G. Grieco and D. Brumley, “Efficient Crash Triage with Black-box Dependency Inference”, submitted for publication.
13. I. Gotovchits, T. Bao, and D. Brumley, “Primus: Memory Check with Micro Execution”, submitted for publication.
14. T. Bao, “Autonomous Computer Security Game: Techniques, Strategy and Investigation”, Doctor of Philosophy Thesis.
15. T. Bao, and Y. Shoshitaishvili, “Game Theory and Machine Learning for Cyber Security” (Book Chapter).

**Professional Activities**

Program Committee

The Network and Distributed System Security Symposium (NDSS) 2020, 2021.

The ACM SIGSAC Conference on Computer and Communications (CCS) 2020.

International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2020.

Annual Computer Security Applications Conference (ACSAC) 2019, 2020.

Workshop on Binary Analysis Research (BAR) 2018, 2019, 2020.

ACM Workshop on Automotive and Aerial Vehicle Security 2020.

Organizing Committee

The IEEE Symposium on Security and Privacy (S&P) 2020.

Journal Reviewer

ACM Transactions on information and System Security. Communications of the ACM.

IEEE Transactions on Software Engineering.

IEEE Transactions on Knowledge and Data Engineering.

Contributor

Introduction to Algorithm and Olympiad in Informatics.

ISBN:9787302291077.

Network Hacking and Defense.

ISBN: 9787121138027.

Hacking Activities

Member of the Order of Overflow, the organization of DEF CON CTF 2018, 2019, 2020.

Open Source Contribution

Mentor of Google Summer of Code, 2013.

**Collaborators and Advisees**

Collaborators and Co-Editors

Ahn, Gail-Joon; Avgerinos, Thanassis; Brumley, David; Dumitras, Tudor; Burket, Jonathan; Doupé, Adam; Gotovchits, Ivan; Kalantari, Faezeh; Kapravelos, Alexandros, Kokulu, Faris Bugra; Kruegel, Christopher; Nelson, Connor; Rubio-Medrano, Carlos; Shoshitaishvili, Yan; Su, Purui; Suciu, Octavian; Sun, Zhibo; Turner, Rafael; Vigna, Giovanni; Wang, Ruoyu; Wang, Yanhao; Woo, Maverick; Zhuge, Jiangwei; Zhao, Ziming.

PhD Committee Chair

Kyle Zeng (expected graduation Spring 2024).

Gokul Menon (expected graduation Spring 2024).

Siyu Liu (expected graduation Spring 2024).

PhD Committee Co-chair

|  |  |  |
| --- | --- | --- |
| Fangzhou Dong.  Ananta Soneji.  Gokul Menon.  Kyle Zheng.  Siyu Liu.  Sukwha Kyung. | Erik Trickel.  Faezeh Kalantari.  Haehyun Cho.  Mehrnoosh Zaeifi.  Penghui Zhang.  Yeganeh Ladwig. | Maxfield Lehman.  Adam Oest.  Faris Kokulu.  Zhibo Sun.  Sana Habib.  Connor Nelson. |

MS Advisee

Yoenjung Lee.

Undergraduate Advisee

Ananay Arora.

Jinxin Hu.