Tiffany Bao

Assistant Professor, Arizona State University, tbao@asu.edu

Education

2018, PhD in Carnegie Mellon University.
Advisor: David Brumley

Selected Academic Publications

Full Publications are listed in https://www.tiffanybao.com/cv.pdf

- Toss a Fault to Your Witcher: Applying Grey-box Coverage-Guided Mutational Fuzzing to Detect SQL and Command Injection Vulnerabilities
  To appear in Proceedings of the IEEE Symposium on Security and Privacy (Oakland '23)
- Playing for K(H)eaps: Understanding and Improving Linux Kernel Exploit Reliability
  The 31st USENIX Security Symposium (USENIX '22) Code Available
- Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs
  The 31st USENIX Security Symposium (USENIX '22) Code Available
- Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits
  The 31st USENIX Security Symposium (USENIX '22)
- "Flawed, but like democracy we don't have a better system": The Experts' Insights on the Peer Review Process of Evaluating Security Papers
  Proceedings of the IEEE Symposium on Security and Privacy (Oakland '22)
- Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service
  The 30th USENIX Security Symposium (USENIX '21)
- CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing
  Proceedings of the 42nd IEEE Symposium on Security and Privacy (Oakland '21)
  Best Student Paper Award
- Favocado: Fuzzing Binding Code of JavaScript Engines Using Semantically Correct Test Cases.
  The Network and Distributed System Security Symposium (NDSS '21) Code Available
- Cyber Autonomy in Software Security: Techniques and Tactics (Book Chapter)
  Game Theory and Machine Learning for Cyber Security (Publisher: Wiley)
- HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems
  Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20) Code Available
- Not All Coverage Measurements Are Equal: Fuzzing by Coverage Accounting for Input Prioritization
  The Network and Distributed System Security Symposium (NDSS '20) Code Available
- Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues
  Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)
- Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits.
  Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland '17)
- How Shall We Play a Game: A Game-theoretical Model for Cyber-warfare Games
  Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF '17)
  The NSA's Annual Best Scientific Paper Award
- ByteWeight: Learning to Recognize Functions in Binary Code
  Proceedings of the 23rd USENIX Security Symposium (USENIX '14) Code Available

Other Contributions

Discover and responsible disclosed more than 30 zero-day vulnerabilities.
Member of the Order Of Overflow, the formal DEF CON CTF organizer 2018-2021
Various program committees (Usenix Security, IEEE Security & Privacy, ACM CCS, NDSS, AAAI)