Yinzhi Cao

yinzhi.cao@jhu.edu
http://yinzhicao.org/
(847)858-8272

Department of Computer Science
The Johns Hopkins University
Baltimore, MD 21210

Research Interests

Cyber security and privacy issues in Web, Mobile, Machine Learning and Payment Systems.

Professional Experience

Assistant Professor *2018.8–Present*
The Johns Hopkins University, Baltimore, MD

Assistant Professor *2015.8–2018.8*
Lehigh University, Bethlehem, PA

Postdoctoral Scientist for Prof. Junfeng Yang *2014.8–2015.7*
Columbia University, New York City, NY

Research Assistant for Prof. Yan Chen *2008.9–2014.7*
Northwestern University, Evanston, IL

Assistant Specialist for Prof. Giovanni Vigna and Prof. Christopher Kruegel *2013.6–2013.9*
UC Santa Barbara, Santa Barbara, CA

Student Associate for Phillip Porras and Vinod Yegneswaran *2011.5–2011.8*
SRI International, Menlo Park, CA

Research Assistant for Prof. Lin Zhang *2007.9–2008.7*
Tsinghua University, Beijing, China

Summer Intern *2007.7–2007.8*
ECCOM Network System Co. Ltd., a Cisco Gold Certificated Partner, Shanghai, China

Student Research Training (SRT) for Prof. Jia Liu *2006.9–2007.7*
Tsinghua University, Beijing, China

Education

PhD in Computer Science (GPA: 3.97/4) *2008.9–2014.6*
Advised by Prof. Yan Chen
Northwestern University, Evanston, IL

Bachelor of Engineering in Electronic Engineering (Major GPA: 89.5/100, top 10%) *2004.9–2008.7*
Tsinghua University, Beijing, China

Publications

Journal and Conference Publications:

1) Practical Blind Membership Inference Attack via Differential Comparisons,
Bo Hui*, Yuchen Yang*, Haolin Yuan*, Philippe Burlina, Neil Gong, and **Yinzhi Cao**,
to appear in the Proceedings of Network & Distributed System Security Symposium (NDSS), 2021.
* First three authors have equal contributions to the paper.

2) *JSKernel: Fortifying JavaScript against Web Concurrency Attacks via a Kernel-like Structure*,
Zhanhao Chen and **Yinzhi Cao**,
in The Annual IEEE/IFIP International Conference on Dependable Systems and Network (DSN), 2020.

3) *Who Touched My Browser Fingerprint? A Large-scale Measurement Study and Classification of Fingerprint Dynamics*
Song Li and **Yinzhi Cao**,
in The ACM Internet Measurement Conference (IMC), 2020 (Long Paper, 38 (Long) +16 (short) / 216 = 24.5%).

4) *Enhancing State-of-the-art Classifiers with API Semantics to Detect Evolved Android Malware*,
Xiaohan Zhang, Yuan Zhang, Ming Zhong, Daizong Ding, **Yinzhi Cao**, Yukun Zhang, Mi Zhang, and Min Yang,
in the Proceedings of The ACM Conference on Computer and Communications Security (CCS), 2020.

5) *PatchAttack: A Black-box Texture-based Attack with Reinforcement Learning*,
Chenglin Yang, Adam Kortylewski, Cihang Xie, **Yinzhi Cao**, and Alan Yuille,
in the Proceedings of European Conference on Computer Vision (ECCV), 2020.

6) *An Ever-evolving Game: Evaluation of Real-world Attacks and Defenses in Ethereum Ecosystem*,
Shunfan Zhou, Zhemin Yang, Jie Xiang, **Yinzhi Cao**, Min Yang, and Yuan Zhang,
in the Proceedings of USENIX Security Symposium, 2020.
Passed Artifact Evaluation.

7) *TextExerciser: Feedback-driven Text Input Exercising for Android Applications*,
Yuyu He, Lei Zhang, Zhemin Yang, **Yinzhi Cao**, Keke Lian, Shuai Li, Wei Yang, Zhibo Zhang, Min Yang, Yuan Zhang, and Haixin Duan,
in the IEEE Symposium on Security and Privacy (Oakland), 2020.

8) *TKPERM: Cross-platform Permission Knowledge Transfer to Detect Overprivileged Third-party Applications*,
Faysal Hossain Shezan, Kaiming Cheng, Zhen Zhang, **Yinzhi Cao**, and Yuan Tian,
in the Proceedings of Network & Distributed System Security Symposium (NDSS), 2020.

9) *Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting*,
Shujiang Wu, Song Li, Yinzhi Cao, and Ningfei Wang,
in the Proceedings of USENIX Security Symposium, 2019 (25/254 = 9.8%, fall submission).

10) *Towards a Secure Zero-rating Framework with Three Parties*,
Zhiheng Liu, Zhen Zhang, **Yinzhi Cao**, Zhaohan Xi, Shihao Jing, and Humberto La Roche,
in the Proceedings of USENIX Security Symposium , 2018 (100/524 = 19%).

11) *FlowCog: Context-aware Semantics Extraction and Analysis of Information Flow Leaks in Android Apps,*
Xiang Pan, **Yinzhi Cao**, Xuechao Du, Boyuan He, Gan Fang, and Yan Chen,
to appear in the Proceedings of USENIX Security Symposium, 2018 (100/524 = 19%).

12) *Efficient Repair of Polluted Machine Learning Systems via Causal Unlearning,*
Yinzhi Cao, Alexander Fangxiao Yu, Andrew Aday, Eric Stahl, Jon Merwine and Junfeng Yang,
in the Proceedings of ACM ASIA Conference on Computer & Communications Security (ASIACCS), 2018

(62/310 = 20%).

13) *DeepXplore: Automated Whitebox Testing of Deep Learning Systems,*
Kexin Pei, **Yinzhi Cao**, Junfeng Yang, and Suman Jana,
in the Proc. of the 26th ACM Symposium on Operating Systems Principles (SOSP), 2017 (39/232 = 16.8%).
This system is reported by Sohu, Jiqizhixin, and ScienceDaily.
Won the **best paper award**.

14) *Deterministic Browser,*
Yinzhi Cao, Zhanhao Chen, Song Li, and Shujiang Wu,
in the Proc. of The ACM Conference on Computer and Communications Security (CCS), 2017 (151/836 = 18%).

15) *(Cross-)Browser Fingerprinting via OS and Hardware Level Features,*
Yinzhi Cao, Song Li, and Erik Wijmans,
in the Proc. of Network & Distributed System Security Symposium (NDSS), 2017 (68/423=16.1%).
This system is released open source and reported by many media outlets, such as BeepingComputer, Hacker's News, and ScienceDaily.

16) *CSPAutoGen: Black-box Enforcement of Content Security Policy upon Real-World Websites,*
Xiang Pan, **Yinzhi Cao**, Shuangping Liu, Yu Zhou, Yan Chen, and Tingzhe Zhou,
in the Proc. of The ACM Conference on Computer and Communications Security (CCS), 2016 (137/837 = 16.4%).

17) *SafePay: Protecting against Credit Card Forgery with Existing Magnetic Card Readers*,
Yinzhi Cao, Xiang Pan and Yan Chen,
in the IEEE Conference on Communications and Network Security (CNS), 2015 (48/171 = 28.1%).
Won the **best paper award**.

18) *Uranine: Real-time Privacy Leakage Monitoring without System Modification for Android*,
Vaibhav Rastogi, Zhengyang Qu, Jedidiah McClurg, **Yinzhi Cao**, and Yan Chen,
in the Proc. of 11th International Conference on Security and Privacy in Communication Networks (SecureComm), 2015 (30/108 = 27.8%).

19) *Towards Making Systems Forget with Machine Unlearning*,
Yinzhi Cao, and Junfeng Yang,
in the Proceeding of the IEEE Symposium on Security and Privacy (Oakland), 2015 (55/407 = 13.5%).
The research is featured by The Stack.

20) *Vetting SSL Usage in Applications with SSLINT*,
Boyuan He, Vaibhav Rastogi, **Yinzhi Cao**, Yan Chen, V.N. Venkatakrishnan, Runqing Yang and Zhenrui Zhang,
in the Proceeding of the IEEE Symposium on Security and Privacy (Oakland), 2015 (55/407 = 13.5%).

21) *EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework*,
Yinzhi Cao, Yanick Fratantonio, Antonio Bianchi, Manuel Egele, Christopher Kruegel, Giovanni Vigna and Yan Chen.
in the Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2015 (50/313 = 15.9%).

22) *TrackingFree: A Next-generation Browser to Protect Users from Third-Party Web Tracking*,
Xiang Pan, **Yinzhi Cao** and Yan Chen.
in the Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2015 (50/313

= 15.9%).

23) *JShield: Towards Real-time and Vulnerability-based Detection of Polluted Drive-by Download Attacks*,
Yinzhi Cao, Xiang Pan, Yan Chen and Jianwei Zhuge.
in the Proceeding of the Annual Computer Security Applications Conference (ACSAC), 2014 (47/236=19.9%).

24) *Protecting Web Single Sign-on against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel*,
Yinzhi Cao, Yan Shoshitaishvili, Kevin Borgolte, Christopher Kruegel, Giovanni Vigna and Yan Chen,
in the Proceeding of International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2014 (22/113=19.5%).

25) *Abusing Your Browser Address bar for Fun and Profit - An Empirical Investigation of Add-on Cross Site Scripting Attacks*,
Yinzhi Cao, Chao Yang, Vaibhav Rastogi, Yan Chen and Guofei Gu,
in the Proceeding of 10th International Conference on Security and Privacy in Communication Networks (SecureComm), 2014.

26) *Redefining Web Browser Principals with a Configurable Origin Policy*,
Yinzhi Cao, Vaibhav Rastogi, Zhichun Li, Yan Chen, and Alex Moshchuk,
in the Proceeding of The Annual IEEE/IFIP International Conference on Dependable Systems and Network - Dependable Computing and Communications Symposium (DSN - DCCS), 2013 (21/107=19.6%).

27) *De-obfuscation and Detection of Malicious PDF Files with High Accuracy*,
Xun Lu, Jianwei Zhuge, Ruoyu Wang, **Yinzhi Cao** and Yan Chen,
in the Proceeding of Hawaii International Conference on System Sciences (HICSS), 2013.

28) *PathCutter: Severing the Self-Propagation Path of XSS JavaScript Worms in Social Web Networks*,
Yinzhi Cao, Vinod Yegneswaran, Phil Porras and Yan Chen,
in Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2012 (46/258=17.8%).

29) *Rake: Semantics Assisted Network-based Tracing Framework*,
Yao Zhao, **Yinzhi Cao**, Yan Chen, Ming Zhang and Anup Goyal,
in IEEE Trans. on Network and Service Management (TNSM), 2012.

30) *Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security*,
Yinzhi Cao, Zhichun Li, Vaibhav Rastogi, Yan Chen and Xitao Wen,
in the Proceeding of ACM Symposium on Information, Computer and Communications Security (ASI-ACCS), 2012 (35/159=22%, full paper).

31) *WebShield: Enabling Various Web Defense Techniques without Client Side Modifications*,
Zhichun Li, Yi Tang, **Yinzhi Cao**, Vaibhav Rastogi, Yan Chen, Bin Liu and Clint Sbisa,
in Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2011 (28/139=20%).

32) *Rake: Semantics Assisted Network-based Tracing Framework*,
Yao Zhao, **Yinzhi Cao**, Anup Goyal, Yan Chen and Ming Zhang,
in Proceeding of International Workshop on Quality of Service (IWQoS), 2011 (23/80=28.8%).

POSTER PUBLICATIONS:

1) *POSTER: A Path-cutting Approach to Blocking XSS Worms in Social Web Networks*,
Yinzhi Cao, Vinod Yegneswaran, Phil Porras and Yan Chen,
poster paper in Proceeding of ACM Conference on Computer and Communications Security (CCS), 2011.

2) *Virtual Browser: a Web-Level Sandbox to Protect Third-Party JavaScript without Sacrificing Functionality*, **Yinzhi Cao**, Zhichun Li, Vaibhav Rastogi and Yan Chen,
poster paper in Proceeding of ACM Conference on Computer and Communications Security (CCS), 2010.

SELECT MEDIA COVERAGE

Newsweekly (Article) *Robots with Artificial Intelligence Become Racist and Sexist—Scientists Think They've Found a Way to Change Their Minds*, October 2017

TechXplore (Article) *Researchers unveil tool to debug 'black box' deep learning algorithms*, October 2017

The Next Web (Article) *Science may have cured biased AI*, October 2017

IEEE Spectrum (Article) *Browser Fingerprinting Tech Works Across Different Browsers for the First Time*, February 2017

Ars Technica (Article) *Now sites can fingerprint you online even when you use multiple browsers – Online tracking gets more accurate and harder to evade*, February 2017

BeepingComputer (Article) *New Fingerprinting Techniques Identify Users Across Different Browsers on the Same PC*, January 2017

The Atlantic (Article) *Machine Unlearning: A possible crack in the brain-computer analogy*, March 2016

EurekAlert! (Article) *New 'machine unlearning' technique wipes out unwanted data quickly and completely*, March 2016

NSF Science Now (Video) *Episode 38 (1'26"–2'58", the second in a 6'17" video with five stories)*, Oct 2015

CCTV America and CCTV News (Video and Interview) *Computer Science expert Yinzhi Cao on new credit card technology*, Oct 2015

NSF Science360 News (Article) *First anti-fraud system to use existing credit card readers*, Sept 2015

Yahoo! News (Article) *New 'SafePay' method to prevent credit card fraud*, Sept 2015

Tech News Today (Article) *SafePay: Unique Adaptive Method Discovered to Prevent Fraud in Card Transactions*, Sept 2015

The Stack (Article) *Machine unlearning: how can information be 'forgotten' in the age of viral data spread?*, Sept 2015

RESEARCH GRANTS

US FUNDING (Total: $2,796,327, My share:$2,196,259)

- GAMEPLAY: Graph Analysis for Mechanized Exploit generation and Patching Leveraging human Assistance for improved Yield, DARPA (subcontracted from UIC), 12/2018–05/2022, $785,611, Single PI at Hopkins.
- SaTC: CORE: Small: Preventing Web Side-channel Attacks via Atomic Determinism (Pending, Recommended for funding), 09/2018–08/2021, $500,000, Single PI at Hopkins.
- Cross-browser Fingerprinting: Attacks, Dynamics, and Detection, Amazon ARA Award, 02/2018–02/2019, $80,000+$20,000 (Amazon Credits), Single PI at Hopkins.
- TWC: Medium: Collaborative: Efficient Repair of Learning Systems via Machine Unlearning, NSF CNS-1563843, 09/2016–08/2021, $1,199,999 (my share $599,931), joint grant with Columbia University, Single PI at Hopkins/Lehigh (REU Supplement: $16,000).
- EAGER: Real-time Enforcement of Content Security Policy upon Real-world Websites, NSF CNS-1646662, 09/2016–08/2017, $94,718, Single PI at Lehigh.
- Privacy-preserving Inspection of Encrypted Traffic via Multi-party, Cross-layer Meta-data Communication, Cisco, 09/2016-08/2017, $99,999, Single PI at Lehigh.

SYNERGISTIC ACTIVITIES

Program Committee Member for

- Annual IEEE/IFIP International Conferece on Dependable Systems and Networks (DSN), 2021, 2020.
- USENIX Security Symposium, 2021, 2020, 2019, 2018.
- The World Wide Web Conference (WWW), Security and Privacy Track, 2018.
- ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2018.
- The ACM Conference on Computer and Communications Security (CCS), 2021,2020,2019,2018, 2017, 2016.
- The IEEE Conference on Communications and Network Security (CNS), 2016, 2015, 2014.
- International Conference on Security and Privacy in Communication Networks (SecureComm), 2020, 2015.

Publications Chair for

- International Conference on Security and Privacy in Communication Networks (SecureComm), 2015.

Web Chair for

- The 1st International Workshop on Security in Embedded Systems and Smartphones (SESP), 2013.

Panelist for

- NSF SaTC, 2020, 2019, 2017.

Journal Reviewer for

- IEEE Transactions on Knowledge and Data Engineering, 2017.
- IEEE Transactions on Mobile Computing, 2017, 2015.
- IEEE Transactions on Information Forensics & Security (TIFS), 2020, 2017, 2012.
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2015, 2014, 2013.
- Applied Computing and Informatics (ACI), 2013.
- IBM Journal of Research and Development, 2015.
- International Journal of Environmental Research and Public Health, 2015.
- Computers and Security, 2015.

External Reviewer for

- ACM Conference on Data and Applications Security (CODASPY), 2017.
- The ACM Conference on Computer and Communications Security (CCS), 2014.
- USENIX Security, 2014.
- IEEE Symposium on Security and Privacy (Oakland), 2016, 2013.
- IEEE INFOCOM, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009.
- IEEE Vehicular Technology Conference (VTC), 2011-Fall.
- The International Workshop on Security in Computers, Networking and Communications (SCNC), 2011.
- Network & Distributed System Security Symposium (NDSS), 2015, 2014, 2012, 2011, 2010.
- The 40th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2010.
- ACM/IEEE International Symposium on Quality of Service (IWQoS), 2013, 2010.
- International Conference on Security and Privacy in Communication Networks (SecureComm), 2011, 2010.
- ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2014, 2013, 2012.
- International Conference on Distributed Computing Systems (ICDCS), 2011.

Volunteer for

- ACM Conference on Computer and Communication Security (CCS), 2011, 2010, 2009.

RESEARCH ADVISING

- PhD Students:

  - Shujiang Wu (Johns Hopkins University,, Advisor, 09/2016–now)
  - Song Li (Johns Hopkins University, Advisor, 09/2017–now)
  - Zifeng Kang (Johns Hopkins University, Advisor, 09/2019–now)
  - Jianjia Yu (Johns Hopkins University, Advisor, 09/2020–now)
  - Bo Hui (Johns Hopkins University, Advisor, 04/2020–now)
  - Yuchen Yang (Johns Hopkins University, Advisor, 04/2020–now)
  - Mingqing Kang (Johns Hopkins, Advisor, 09/2020–now),
  - Neil Fendley (JHU/APL, Advisor, 09/2020–now).

  - Zhen Zhang (Lehigh University, Advisor, 09/2017–08/2019)
  - Dan Luo (Lehigh University, Co-advisor, 09/2017–05/2020)
  - Hongfa Ding (Guizhou University, visiting Ph.D student, 10/2017–08/2018)
  - Xiang Pan (Northwestern University, Thesis Committee Member, 09/2012–08/2017)
  - Tingzhe Zhou (Lehigh University, Course Instructor, 01/2016–05/2016)
- MS Students:
  - Haolin Yuan (Johns Hopkins University, Advisor, 04/2020–now)
  - Song Li (Financially supported, Lehigh, mentored from 12/2015–08/2017),
  - Zhanhao Chen (Financially supported, Lehigh, mentored from 10/2016–08/2018, went to Palo Alto Networks as a researcher),
  - Zhiheng Liu (Lehigh University, Advisor, 09/2016–08/2018, went to Microsoft)
  - Varun Nagender Sharma (Lehigh, mentored from 01/2015–07/2015),
  - Ji Qi (UT-Dallas, summer intern, mentored from 05/2016–08/2016),
  - James Lamberti (Lehigh, mentored from 02/2016–06/2016).
  - Vishal Vyas (Columbia, mentored from 09/2014–07/2015),
  - Diwakar Mahajan (Columbia, mentored from 09/2014–12/2014),
  - Qiming Chen (Columbia, mentored from 09/2014–12/2014),
  - Chang Chen (Columbia, mentored from 09/2014–12/2014).
- Undergraduate:
  - Eric Stahl (Lehigh, mentored from 01/2016–06/2016, graduated and admitted by UPenn)
  - Olivia Orrell-Jones (Brown University, REU student from 05/2017–07/2017)
  - Erik Wijmans (Washington University in St. Louis, REU Students from 05/2016–07/2016, admitted by George Tech as a Ph.D. student with my recommendation)
  - Jinquan Zhang (Zhejiang University, visiting students from 05/2016–10/2016)
  - Alex Yang (Columbia, mentored from 05/2015–09/2015)
  - Alex Yu (Columbia, mentored from 05/2015–08/2015)
  - Andrew Aday (Columbia, mentored from 09/2015–02/2016)

TEACHING EXPERIENCE

Instructor *Spring 2021*
EN 740: Language-based Security, Johns Hopkins University

Instructor *Fall, 2020*
EN 340/440/640: Web Security, Johns Hopkins University

Instructor *Fall, 2019*
EN 340/440/640: Web Security, Johns Hopkins University

Instructor *Fall, 2018*

EN 340/440/640: Web Security, Johns Hopkins University

Instructor *Fall, 2017*
CSE 303: Operating System Design, Lehigh University

Instructor *Spring, 2017*
CSE 403: Advanced Operating Systems, Lehigh University
Teaching Evaluation Score (Overall): 4.69/5

Instructor *Fall, 2016*
CSE 350/450: Cyber Defense and Offense, Lehigh University
Teaching Evaluation Score (Overall): 3.71/5

Guest Lecturer *Fall, 2016*
CSE 406: Research Methods, CSE 411: Advanced Programming Techniques, and CSE 342: Fundamentals of Internetworking

Instructor *Spring, 2016*
CSE 403: Advanced Operating Systems, Lehigh University
Teaching Evaluation Score (Overall): 4.33/5

Instructor *Fall, 2015*
CSE 343/443: Network Security, Lehigh University
Teaching Evaluation Score (Overall): 4/5

Guest Lecturer *Fall, 2015*
CSE 252: Computer Society and Internet, CSE 406: Research Methods, CSE 411: Advanced Programming Techniques, and CSE 424: Advanced Communication Networks

Project Mentor *Fall, 2015*
CSE 379: Senior Project, Lehigh University

Project Grader *Fall, 2015*
ECE 257: Senior Design, Lehigh University

Guest Lecturer on Web Security *Fall, 2014*
E6121: Reliable Software, Columbia University.

Teaching Assistant *Spring, 2014*
EECS 230: Programming for Engineers, Northwestern University
CTEC (Course and Teacher Evaluation Council) Score: 5.545/6

Students Group Project Mentor on Java 0-day Vulnerability *Fall, 2013*
EECS 354: Network Penetration and Security, Northwestern University
Group Member: Glenn Fellman, Audrey Hosford, Scott Neaves and Sam Toizer.

Guest Speaker on Web Security & Students Group Project Mentor on Credit Card Security *Winter, 2013*
EECS 450: Internet Security, Northwestern University
Group Member: Titi Gu and Yiyang Yang.

Students Group Project Mentor on Malicious URL Analysis *Fall, 2012*
EECS 354: Network Penetration and Security, Northwestern University
Group Member: Christopher Charles Moran, Peter Meng Li and Ethan Romba.

Guest Speaker on Web Security *Spring, 2012*

EECS 450: Internet Security, Northwestern University

Teaching Assistant *Winter, 2012*
EECS 211: Object-Oriented Programming in C++, Northwestern University
CTEC Score: 5.25/6 (Section One) 5.5/6 (Section Two)

Teaching Assistant *Fall, 2011*
EECS 354 - Network Penetration and Security, Northwestern University
CTEC Score: 5/6

Teaching Assistant *Fall, 2010*
Engineering Analysis - I, Northwestern University
CTEC Score: N/A

Patent

De-obfuscation and Signature Matching Technologies for Detecting Malicious Code,
Yinzhi Cao, Xiang Pan, Yan Chen, Jianwei Zhuge, Xiaobin Qian, and Jian Fu,
filed on March 13, 2014, allowed on October 7, 2015, under US Patent Application No. 14/207,665.

Invited Talks

1) *Web Tracking: Attacks and Defenses*,
Invited talk at Tsinghua University, China, June 2017.
Invited talk at University of Science and Technology of China (USTC), June 2017.

2) *Towards a secure zero-rating framework with three parties*,
Invited talk at Zhejiang University, June 2017.
Invited talk at Cisco, June 2017.

3) *Towards Making System Forget*,
Invited talk at JHU/APL, April 2019.
Invited talk at AT&T Bell Labs, August 2016.
Invited talk at Northwestern University, March 2016.
Invited talk at University of Chicago, January 2016.
Invited talk at NYU-Poly, October 2015.
Invited lightening talk at DTL Conference, October 2015.
Invited talk at Georgia Institute of Technology, April 2015.
Invited talk at NYU, April 2015.

4) *Enhancing System Security and Privacy with Program Analysis*,
Invited talk at IBM TJ Watson, April 2015.
Invited talk at Purdue University, April 2015.
Invited talk at Worcester Polytechnic Institute, March 2015.
Invited talk at VirginiaTech, March 2015.
Invited talk at University of Maryland–Baltimore County, March 2015.
Invited talk at Stevens Institute of Technology, March 2015.
Invited talk at University of Delaware, March 2015.
Invited talk at University of Iowa, March 2015.
Invited talk at Iowa State University, February 2015.
Invited talk at Penn State University, February 2015.
Invited talk at University of Nebraska–Lincoln, February 2015.

Invited talk at Marquette University, January 2015.

5) *Protecting Client Browsers with a Principal-Based Architecture*,
Invited talk at University of New Hampshire, February 2014.
Invited talk at Worcester Polytechnic Institute, February 2014.
Invited talk at Boston University, January 2014.

6) *Introduction to Web Security*,
Invited talk at Huawei Technologies Co. Ltd., Beijing, March 2013.

7) *Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security*,
Invited talk at Network and Information Security Lab of Tsinghua University, Beijing, May 2012.

Services

- BS in CS Redesign Committee, Johns Hopkins University, 2020–2021.
- Curriculum Committee, Johns Hopkins University, 2019–2021.
- Graduate Student Admission Committee, Lehigh University, 2015–2018.
- CS Core Recruiting Committee, Lehigh University, 2015–2018.
- Panelist for Center Valley Forum on the discussion of "Privacy vs. Security: The Battle between Apple and the FBI", DeSales University, March 2016.
- ECE Senior Project Grading Committee, Lehigh University, Fall 2015.
- Invited Orientation Panel Member for *Thriving in Graduate School: Perspectives of Current Students*, Northwestern University, 2010.
- Board Member of Chinese Student and Scholar Association (CSSA), Northwestern University, 2009.

Software Artifacts and Community Contributions

- 68 CVE vulnerabilities on Node.js platform. Most influential ones include CVE-2020-7684, CVE-2020-7682, CVE-2019-10777, CVE-2019-10778, and CVE-2020-7677.
- DeterFox – A prototype implementation of deterministic browser – a browser to defend timing attacks.
  System available at http://www.deterfox.org.
- UniqueMachine – A cross-browser fingerprinting platform.
  System available at http://www.uniquemachine.org.
- EdgeMiner – A static analysis tool that extracts implicit control flow transitions from Android framework.
  System available at http://www.yinzhicao.org/EdgeMiner.
- JShield – Real-time and vulnerability-based detection of polluted drive-by download attacks.
  System adopted by the world's largest telecommunication equipment maker, *Huawei Technologies Co. Ltd.*
- MPScan – Real-time de-obfuscation and detection of malicious PDF files.
  System adopted by the world's largest telecommunication equipment maker, *Huawei Technologies Co. Ltd.*
- Configurable Origin Framework – A modified version of WebKit with configurable origin policy, the next generation access control policy for web browser.
  System available at https://code.google.com/p/configurableoriginpolicy/.
- Virtual Browser – A virtualized browser to sandbox third-party JavaScripts with enhanced security.
  System available upon Request.

Honors

Best Paper Award of ACM SOSP'17	*2017*
Best Paper Award of IEEE CNS'15	*2015*
Terminal Year Fellowship of McCormick School of Engineering	*2013–2014*

Volunteer Awards for ACM Conference on Computer and Communication Security (CCS)	*2009–2011*
Scholarship of Mao Tai, the friend of Tsinghua University	*2006*
Scholarship of Geru Zheng, the friend of Tsinghua University	*2005*
Freshman Scholarship of Tsinghua University	*2004*
2nd in College Entrance Examination of Anhui Province among over 500 thousands students	*2004*
1st rank prize in Physics Olympiad of Anhui Province	*2003*
2nd in Chemistry Olympiad of Anhui Province	*2003*
3rd rank prize in Biology Olympiad of Anhui Province	*2001*
1st in Computing Olympiad of Hefei (the Capital of Anhui Province)	*1997–2000*