Yinzhi Cao

yinzhicao2013@u.northwestern.edu
http://www.cse.lehigh.edu/~yzcao
(847)-858-8272

19 Memorial Drive,
Packard Lab 380,
Bethlehem, PA 18015

PROFESSIONAL EXPERIENCE

Assistant Professor — *2015.8–Present*
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: 3.970/4) — *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 (Authors with * are students under my supervision):

1) *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*,
Yinzhi Cao, Song Li* and Erik Wijmans*,
to appear in the Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2017. (68/423=16.1%)

2) *CSPAutoGen: Blackbox Enforcement of Content Security Policy upon Real-world Websites*,
Xiang Pan*, **Yinzhi Cao**, Shuangping Liu*, Yu Zhou*, Yan Chen, and Tingzhe Zhou*,
in Proceeding of ACM Conference on Computer and Communications Security (CCS), 2016. (137/837 = 16.4%)

3) *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**.

4) *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%)

5) *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.

6) *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%).

7) *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%).

8) *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%).

9) *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%).

10) *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%)

11) *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.

12) *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%)

13) *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.

14) *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%)

15) *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.

16) *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)

17) *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%)

18) *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.

RESEARCH GRANTS

US FUNDING (Total: $1,394,717, My share: $794,649):

- TWC: Medium: Collaborative: Efficient Repair of Learning Systems via Machine Unlearning, NSF CNS-1563843, 09/2016–08/2020, $1,199,999 (my share $599,931), joint grant with Columbia University, Single PI at Lehigh.
- 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, $100,000, Single PI at Lehigh.

OTHERS (Total: RMB 620,000):

- Quantitative Diagnosis of Embedded Software Based on Multi-source Uncertain Noise Resonance, National Natural Science Foundation of China NSFC-61672080, 01/2017–12/2020, RMB 620,000 (around $90,354), Co-PI applied via Beihang University (PI Shunkun Yang).

SELECT MEDIA COVERAGE

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[1] 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,*[2] 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

SYNERGISTIC ACTIVITIES

Program Committee Member for

- The ACM Conference on Computer and Communications Security (CCS), 2016.
- The IEEE Conference on Communications and Network Security (CNS), 2016, 2015, 2014.
- International Conference on Security and Privacy in Communication Networks (SecureComm), 2016, 2015.
- The 2016 IEEE International Conference on Progress in Informatics and Computing (PIC), 2016.

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.

Journal Reviewer for

- IEEE Transactions on Information Forensics & Security (TIFS), 2012.
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2015, 2014, 2013.
- Applied Computing and Informatics (ACI), 2013.
- IEEE Transactions on Mobile Computing, 2015.
- 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.

[1] CCTV, China Central Television, is like "CNN in China".

[2] The article also appears in about 30 other media outlets.

- 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

- Undergraduate:
  - Eric Stahl (Lehigh, mentored from 01/2016–06/2016, graduated and admitted by UPenn)
  - Erik Wijmans (Washington University in St. Louis, REU Students from 05/2016–07/2016)
  - 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)
- MS Students:
  - Song Li (Financially supported, Lehigh, mentored from 12/2015–now),
  - Zhanhao Chen (Financially supported, Lehigh, mentored from 10/2016–now),
  - 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).
- PhD Students:
  - Zhiheng Liu (Lehigh University, Advisor, 09/2016–now)
  - Shujiang Wu (Lehigh University, Advisor, 09/2016–now)
  - Xiang Pan (Northwestern University, Thesis Committee Member, 09/2012–now)
  - Tingzhe Zhou (Lehigh University, Course Instructor, 01/2016–05/2016)

TEACHING EXPERIENCE

Instructor *Spring, 2017*
CSE 403: Advanced Operating System, Lehigh University
Teaching Evaluation Score (Overall): Unavailable

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

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 System, 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[3] 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,

[3] CTEC is short for Course and Teacher Evaluation Council, which provides a confidential survey for each student taking the course. There are four questions for TAs and the score listed is the average of the four questions.

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 (supersedes provisional application No. 61/786,200 on March 14, 2013).

INVITED TALKS

1) *Towards Making System Forget*,
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.

2) *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.

3) *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.

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

5) *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

- PhD Thesis Committee Member:
  - Xiang Pan (Northwestern University)
  - Zhengyang Qu (Northwestern University)
  - Qinghan Xue (Lehigh University)
- Thesis Depth Study Committee Member:
  - Jinbu Wang (Lehigh University)
- Graduate Student Admission Committee, Lehigh University, 2015–present.
- CS Core Recruiting Committee, Lehigh University, 2015–present.

- 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

- 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 AND AWARDS

Travel Grant for DTL Conference (Accept Rate: 34% with 3 page proposal.)	*2015*
Best Paper Award of IEEE CNS	*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*