Yinzhi Cao

yinzhicao2013@u.northwestern.edu
http://www.cs.northwestern.edu/~yca179
(847)-858-8272

2133 Sheridan Road RM 2-207,
Evanston, IL 60208, USA

RESEARCH INTEREST

My current research spans Web security and language based security to network and data center diagnosis. I am also interested in other system and network security topics.

EDUCATION

PhD in Computer Science (GPA: 3.970/4) *2008.9 - 2014.6 (Expected)*
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

PROFESSIONAL EXPERIENCE

Research Assistant for Prof. Yan Chen *2008.9 - Present*
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

PUBLICATION

JOURNAL AND CONFERENCE PUBLICATION:

1) *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%)

2) *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%)

3) *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.

4) *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 (ASIACCS), 2012. (35/159=22%, full paper)

5) *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%)

6) *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%)

7) *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.

POSTER PUBLICATION:

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.

PAPERS UNDER SUBMISSION

1) *JShield: Towards Real-time and Vulnerability-based Detection of Polluted Drive-by Download Attacks*,
Yinzhi Cao, Xiang Pan, Yan Chen and Jianwei Zhuge.

2) *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.

3) *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.

4) *EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework*,
Yinzhi Cao, Yanick Fratantonio, Antonio Bianchi, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Yan Chen and David Brumley.

5) *SafePay: Protecting against Credit Card Forgery with Existing Magnetic Card*,
Yinzhi Cao, Xiang Pan and Yan Chen.

6) *TrackingFree: A Next-generation Browser to Protect Users from Third-Party Web Tracking*,
Xiang Pan, **Yinzhi Cao**, Youfu Zhang and Yan Chen.

SOFTWARE ARTIFACTS

- JShield – Real-time and vulnerability-based detection of polluted drive-by download attacks.
  System adopted by the world largest telecommunication equipment maker, *Huawei Technologies Co. Ltd*.
- MPScan – Real-time de-obfuscation and detection of malicious PDF files.
  System adopted by the world 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

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*

SKILLS

Strong Experience in C/C++, JavaScript, Matlab, Verilog, VHDL, Pascal, DOS, and Linux;
Master Java and PHP;
Knowledgable in WebKit Source Codes.

PROFESSIONAL ACTIVITIES

Program Committee Member for

- the 2nd IEEE Conference on Communications and Network Security (CNS), 2014.

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), 2013.
- Applied Computing and Informatics (ACI), 2013.

External Reviewer for

- IEEE Symposium on Security and Privacy (Oakland), 2013.
- IEEE INFOCOM, 2014, 2013, 2012, 2011, 2010, 2009.
- Network & Distributed System Security Symposium (NDSS), 2014, 2012, 2011, 2010.
- ACM/IEEE International Symposium on Quality of Service (IWQoS), 2013, 2010.
- The 40th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2010.
- International Conference on Distributed Computing Systems (ICDCS), 2011.

- ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2013, 2012.

Volunteer for

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

TEACHING EXPERIENCE

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[1] 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 14, 2013, under U.S. Application No. 61/786,200.

INVITED TALKS

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

2) *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.

PRESENTATIONS

1) *Redefining Web Browser Principals with a Configurable Origin Policy*,
Presented at the Annual IEEE/IFIP International Conference on Dependable Systems and Network - Dependable Computing and Communications Symposium (DSN - DCCS), Budapest, June 2013.

[1] 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.

2) *Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security*,
Presented at ACM Symposium on Information, Computer and Communications Security, Seoul, May 2012.

3) *PathCutter: Severing the Self-Propagation Path of XSS JavaScript Worms in Social Web Networks*
Presented at the Annual Network & Distributed System Security Symposium, San Diego, February 2012.

4) *Rake: Semantics Assisted Network-based Tracing Framework*,
Presented at ACM/IEEE International Workshop on Quality of Service, San Jose, CA, June 2011.

OTHERS

Invited Orientation Panel Member for *Thriving in Graduate School: Perspectives of Current Students*, 2010.
Board Member of Chinese Student and Scholar Association (CSSA) at Northwestern University, 2009.

REFERENCES

- Professor Yan Chen (Advisor at Northwestern University)
Tech Inst. Room L459
2145 Sheridan Road
Evanston, IL 60208
ychen@northwestern.edu
- Professor Giovanni Vigna (Internship Mentor at UC Santa Barbara)
2117 Harold Frank Hall, Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
vigna@cs.ucsb.edu
- Professor Christopher Kruegel (Internship Mentor at UC Santa Barbara)
2117 Harold Frank Hall, Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
chris@cs.ucsb.edu
- Phillip Porras (Internship Mentor at SRI International)
Room EL 219
333 Ravenswood Avenue
Menlo Park, CA 94025
porras@csl.sri.com
- Vinod Yegneswaran (Internship Mentor at SRI International)
Computer Science Laboratory
SRI International
333 Ravenswood Ave
Menlo Park, CA 94025
vinod@csl.sri.com