Yizheng Chen

Postdoctoral Scholar
University of California, Berkeley
Berkeley, CA, USA

+1(805)570-2071
1z@berkeley.edu
Google Scholar

Research Interests

My research focus is **computer security**. I am interested in designing and building robust machine learning systems for security applications. My research goal is to develop robust machine learning techniques to solve real-world security problems with strong theoretical guarantees and high performance, that can increase the economic cost for adaptive attackers to evade detection.

Work Experience

University of California, Berkeley, CA, USA
Postdoctoral Scholar, Advisor: David Wagner — **September 2021 – Current**

Columbia University, New York, NY, USA
Postdoctoral Scholar, Advisor: Suman Jana — **Oct 2018 – August 2021**

Baidu USA, Sunnyvale, CA, USA
Senior Security Researcher — **Nov 2017 – Oct 2018**

Facebook, Menlo Park, CA, USA
Research Intern — **May 2016 – Aug 2016**

Comcast, Atlanta, GA, USA
Research Intern — **May 2015 – Aug 2015**

SRI International, Menlo Park, CA, USA
Research Intern — **May 2014 – Aug 2014**

Damballa Inc., Atlanta, GA, USA
Research Intern — **May – Aug 2012, 2013**

Cisco Research and Development Center, Shanghai, China
Software Engineer Intern — **Mar 2010 – Aug 2010**

Education

Georgia Institute of Technology, Atlanta, GA, United States

Ph.D., Computer Science — **Aug 2011 - Dec 2017**

- Dissertation Topic: Network Security, Applied Machine Learning and Online Advertising Fraud
- Advisors: Wenke Lee and Manos Antonakakis

Fudan University, Shanghai, China

B.S., Information Security — **Sep 2007 - Jul 2011**

University of California, Santa Barbara, CA, United States

Exchange Student, Computer Science, Dean's Honors — **Sep 2009 - Dec 2009**

Publications

7 in top-tier security conferences (*IEEE S&P, USENIX Security, ACM CCS*)

Referred Conference Papers

[1] **Learning security classifiers with verified global robustness properties**.
Yizheng Chen, Shiqi Wang, Yue Qin, Xiaojing Liao, Suman Jana, and David Wagner.
In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* ***(CCS)***, 2021.
∗ **Best Paper Award Runner-Up**
∗ Our training algorithm is available here (https://github.com/surrealyz/verified-global-properties).

[2] **Cost-Aware Robust Tree Ensembles for Security Applications**.
Yizheng Chen, Shiqi Wang, Weifan Jiang, Asaf Cidon, and Suman Jana.
In *USENIX Security Symposium* ***(USENIX Security)***, 2021.
∗ Our robust training algorithm over scikit-learn and XGBoost is here (https://github.com/surrealyz/growtrees).

[3] **On Training Robust PDF Malware Classifiers**.
Yizheng Chen, Shiqi Wang, Dongdong She, and Suman Jana.
In *USENIX Security Symposium* ***(USENIX Security)***, 2020.
∗ Our code and models are available here (https://github.com/surrealyz/pdfclassifier).

[4] **Neutaint: Efficient Dynamic Taint Analysis with Neural Networks**.
Dongdong She, Yizheng Chen, Abhishek Shah, Baishakhi Ray, and Suman Jana.
In *2020 IEEE Symposium on Security and Privacy* ***(IEEE S&P)***, pages 364–380.

[5] **Practical Attacks Against Graph-based Clustering**.
Yizheng Chen, Yacin Nadji, Athanasios Kountouras, Fabian Monrose, Roberto Perdisci, Manos Antonakakis, and Nikolaos Vasiloglou.
In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* ***(CCS)***, 2017.
∗ Top 10 Finalist of the **CSAW'17 Applied Research Competition**.

[6] **Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse**.
Panagiotis Kintis, Najmeh Miramirkhani, Charles Lever, Yizheng Chen, Rosa Romero-Gómez, Nikolaos Pitropakis, Nick Nikiforakis, and Manos Antonakakis.
In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* ***(CCS)***, 2017.
∗ ComboSquatting Clusters (https://www.activednsproject.org/combosquatting.html)
∗ Media Coverage: **Domain Name Wire**, **Georgia Tech**, **EurekAlert!**, **ZDNet**, **Domain Pulse**, **World Trademark Review**, **GIGALAW**, etc.

[7] **Measuring Network Reputation in the Ad-Bidding Process**.
Yizheng Chen, Yacin Nadji, Rosa Romero-Gómez, Manos Antonakakis, and David Dagon.
In *Detection of Intrusions and Malware, and Vulnerability Assessment* ***(DIMVA)***, 2017.

[8] **Enabling Network Security Through Active DNS Datasets**.
Athanasios Kountouras, Panagiotis Kintis, Chaz Lever, Yizheng Chen, Yacin Nadji, David Dagon, Manos Antonakakis, and Rodney Joffe.
In *International Symposium on Research in Attacks, Intrusions, and Defenses* ***(RAID)***, 2016.
∗ **Active DNS Dataset** (https://activednsproject.org/) has been used by 70 research groups from more than 50 organizations, from more than 15 countries.

[9] **Financial Lower Bounds of Online Advertising Abuse**.
Yizheng Chen, Panagiotis Kintis, Manos Antonakakis, Yacin Nadji, David Dagon, Wenke Lee, and Michael Farrell.
In *Detection of Intrusions and Malware, and Vulnerability Assessment* ***(DIMVA)***, 2016.

[10] **On the Feasibility of Large-Scale Infections of iOS Devices**.
Tielei Wang, Yeongjin Jang, Yizheng Chen, Simon P Chung, Billy Lau, and Wenke Lee.
In *USENIX Security Symposium* ***(USENIX Security)***, 2014.
∗ Media Coverage: **The Register**, **Wired**, **Toms Guide**, **ComputerWorld**, **PCWorld**, etc.

[11] **DNS Noise: Measuring the Pervasiveness of Disposable Domains in Modern DNS Traffic**.
Yizheng Chen, Manos Antonakakis, Roberto Perdisci, Yacin Nadji, David Dagon, and Wenke Lee.
In *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* ***(DSN)***, 2014.

Referred Workshop Papers

[12] **SEAT: Similarity Encoder by Adversarial Training for Detecting Model Extraction Attack Queries**.
Zhanyuan Zhang, Yizheng Chen, and David Wagner.
In *Proceedings of the ACM Workshop on Artificial Intelligence and Security* ***(AISec)***, 2021.

[13] **Enhancing gradient-based attacks with symbolic intervals**.
Shiqi Wang, Yizheng Chen, Ahmed Abdou, and Suman Jana.
In *ICML Workshop on Security and Privacy of Machine Learning* ***(SPML)***, 2019.
∗ Oral Presentation at the workshop. **Interval attacks** appear on MadryLab MNIST Challenge Leaderboard. (https://github.com/MadryLab/mnist_challenge).

[14] **FeatNet: Large scale Fraud Device Detection by Network Representation Learning with Rich Features**.
Chao Xu, Zhentan Feng, Yizheng Chen, Minghua Wang, and Tao Wei.
In *Proceedings of the ACM Workshop on Artificial Intelligence and Security* ***(AISec)***, 2018.

Referred Journal Papers

[15] **Measuring Lower Bounds of the Financial Abuse to Online Advertisers: A Four Year Case Study of the TDSS/TDL4 Botnet**.
Yizheng Chen, Panagiotis Kintis, Manos Antonakakis, Yacin Nadji, David Dagon, and Michael Farrell.
Computers & Security, 67:164–180, 2017.

Preprints

[16] **MixTrain: Scalable Training of Formally Robust Neural Networks**.
Shiqi Wang, Yizheng Chen, Ahmed Abdou, and Suman Jana.
arXiv preprint arXiv:1811.02625, 2018.

Academic Service

Organizing Committee

- PC Co-Chair for the 5th Deep Learning and Security Workshop Co-located with IEEE S&P 2022
- PC Co-Chair for the 14th AISec Workshop Co-located with ACM CCS 2021
  We received a record number of 56 paper submissions.

Technical Program Committee Member

- USENIX Security Symposium 2022
- ACM Workshop on Robust Malware Analysis (Co-located with ACM ASIACCS) 2022
- ACM Conference on Computer and Communications Security (CCS) 2021
- ACM Workshop on Artificial Intelligence and Security (AISec) 2019, 2020
- ICLR Workshop on Trustworthy ML 2020
- CVPR Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems 2019
- ICML Workshop on Security and Privacy of Machine Learning 2019
- Neurips Workshop on Security in Machine Learning 2018
- IEEE Deep Learning and Security Workshop 2018, 2019, 2020, 2021

Reviewer

- Journal of Computer Security 2021
- ACM Transactions on Internet Technology 2020
- ACM Transactions on Privacy and Security 2019
- IEEE Transactions on Information Forensics and Security 2019
- Elsevier Computers and Security 2019
- Qualification Round Judge for CSAW Applied Research Competition 2018, 2019
- Wiley Security & Privacy 2018
- IEEE Security and Privacy Journal Special Issue: Digital Forensics 2017

Teaching Experience

Research Mentoring for Master's Student

- Weifan Jiang, Columbia University -> PhD student at Harvard University
  Project: Cost-Aware Robust Tree Ensembles for Security Applications, USENIX Security 2021 [2].

Research Mentoring for Undergraduate Student

- Zeyi (Lucia) Liu, Columbia University -> Applying for PhD program
  Project: MalGAN attack evaluation on robust PDF malware classifiers,
  https://github.com/lzylucy/Malware-GAN-attack.
- Songchen (Sophia) Yao, Columbia University
  Project: Porting EvadeML to AWS.
- Crystal Ren, Columbia University
  Project: PDF malware analysis.

Teaching Assistant for Network Security (Graduate-level) Spring 2012, Fall 2014
Taught project sessions, held office hours, created projects, graded homeworks and projects.

Honors & Awards

ACM CCS Best Paper Award Runner-up [1], 2021.

Google ASPIRE (Android Security and PrIvacy REsearch) Award, $105,000, 2021.

EECS Rising Stars, I was selected to attend the EECS rising stars workshop 2020.

Top 10 Finalist [5], NYU CSAW'17 Applied Research Competition, New York, NY, 2017.

Google Anita Borg Memorial Scholarship, 30 students with the major in computer science or related field are awarded in China, 2010.